

User Manual

GEM420

4G M2M Router



TABLE OF CONTENTS

CHAPTER 1	INTRODUCTION	7
1.1	CONTENTS LIST	8
1.2	HARDWARE INSTALLATION	9
1.2.1	WARNING	9
1.2.2	SYSTEM REQUIREMENTS	9
1.2.3	Hardware Configuration	10
1.2.4	LED Indication	12
CHAPTER 2	GETTING STARTED	13
2.1	HARDWARE INSTALLATION	13
2.1.1	Mount the Unit	13
2.1.2	Insert the SIM Card	13
2.1.3	Connecting Power	14
2.1.4	Connecting to the Network or a Host	14
2.2	EASY SETUP BY CONFIGURING WEB UI	15
2.2.1	Wizard	15
2.2.2	Status	23
CHAPTER 3	MAKING CONFIGURATIONS	28
3.1	BASIC NETWORK	30
3.1.1	WAN Setup	31
3.1.1.1	Physical Interface	32
3.1.1.2	Internet Setup	34
3.1.1.2.1	3G/4G WAN – 3G/4G	34
3.1.1.2.2	Ethernet WAN	38
3.1.1.3	Load Balance	51
3.1.2	LAN & VLAN Setup	53
3.1.2.1	Ethernet LAN	54
3.1.2.2	VLAN	55
3.1.2.2.1	VLAN Scenarios	55
3.1.2.2.2	Port-Based VLAN	59
3.1.2.2.3	Tag-Based VLAN	61
3.1.3	WiFi Setup	62
3.1.3.1	WiFi Configuration	63
3.1.3.1.1	AP Router Mode	63
3.1.3.1.2	WDS Only Mode	67

3.1.3.1.3	WDS Hybrid Mode	70
3.1.3.1.4	WPS Setup	73
3.1.3.2	Wireless Client List.....	74
3.1.3.3	Advanced Configuration	75
3.1.4	IPv6 Setup	77
3.1.4.1	Static IPv6.....	78
3.1.4.2	DHCP v6	80
3.1.4.3	PPPoEv6.....	82
3.1.4.4	6 to 4	83
3.1.4.5	6 in 4	85
3.1.5	NAT / Bridging	86
3.1.5.1	Configuration.....	87
3.1.5.2	Virtual Server & Virtual Computer	87
3.1.5.2.1	Virtual Server	87
3.1.5.2.2	Virtual Computer.....	88
3.1.5.2.3	Special AP & ALG	88
3.1.5.3	DMZ	89
3.1.6	Routing Setup.....	90
3.1.6.1	Static Routing.....	90
3.1.6.2	Dynamic Routing.....	91
3.1.6.3	Routing Information.....	94
3.1.7	Client/Server/Proxy	95
3.1.7.1	Dynamic DNS	95
3.1.7.2	DHCP Server	96
3.2	ADVANCED NETWORK.....	99
3.2.1	Firewall	100
3.2.1.1	Configuration.....	100
3.2.1.2	Packet Filters	100
3.2.1.2.1	Configuration	101
3.2.1.2.2	Packet Filter List	101
3.2.1.2.3	Packet Filter Rule Configuration.....	102
3.2.1.3	URL Blocking	103
3.2.1.3.1	Configuration	104
3.2.1.3.2	URL Blocking Rule List.....	104
3.2.1.3.3	URL Blocking Rule Configuration.....	105
3.2.1.4	Web Content Filters	105
3.2.1.4.1	Configuration	106
3.2.1.4.2	Web Content Filter Rule List.....	106

3.2.1.4.3	Web Content Filter Configuration	107
3.2.1.5	MAC Control	107
3.2.1.5.1	Configuration	108
3.2.1.5.2	MAC Control Rule List.....	108
3.2.1.5.3	MAC Control Rule Configuration.....	109
3.2.1.6	Application Filters.....	109
3.2.1.6.1	Configuration	110
3.2.1.7	IPS	110
3.2.1.8	Options.....	111
3.2.2	QoS & BWM	112
3.2.2.1	Configuration.....	113
3.2.2.2	Rule-based QoS	114
3.2.2.2.1	Configuration	115
3.2.2.2.2	QoS Rule List.....	115
3.2.2.2.3	QoS Rule Configuration.....	116
3.2.3	VPN Setup.....	120
3.2.3.1	IPSec	121
3.2.3.1.1	IPSec VPN Tunnel Scenarios	121
3.2.3.1.2	IPSec Configuration	123
3.2.3.1.3	Tunnel List & Status.....	124
3.2.3.1.4	Local & Remote Configuration	124
3.2.3.1.6	Authentication	125
3.2.3.1.7	IKE Phase.....	125
3.2.3.1.8	IKE Proposal Definition.....	126
3.2.3.1.9	IPSec Phase	127
3.2.3.1.10	IPSec Proposal Definition	127
3.2.3.1.11	Manual Proposal.....	128
3.2.3.2	PPTP.....	128
3.2.3.2.1	PPTP / L2TP VPN Tunnel Scenarios.....	129
3.2.3.2.2	PPTP Server Configuration	130
3.2.3.2.3	PPTP Server Status.....	131
3.2.3.2.4	User Account List.....	131
3.2.3.2.5	User Account Configuration.....	132
3.2.3.2.6	PPTP Client	132
3.2.3.2.7	PPTP Client List & Status	132
3.2.3.2.8	PPTP Client Configuration.....	133
3.2.3.3	L2TP	134
3.2.3.3.1	L2TP Server Configuration	134

3.2.3.3.2	L2TP Server Status.....	135
3.2.3.3.3	User Account List.....	136
3.2.3.3.4	User Account Configuration.....	136
3.2.3.3.5	L2TP Client.....	136
3.2.3.3.6	L2TP Client List & Status	137
3.2.3.3.7	L2TP Client Configuration.....	137
3.2.3.4	GRE	138
3.2.3.4.1	GRE VPN Tunnel Scenario.....	138
3.2.3.4.2	GRE Configuration	139
3.2.3.4.3	GRE Tunnel Definitions.....	139
3.2.3.4.4	GRE rule Configuration	140
3.2.4	Redundancy	141
3.2.4.1	VRRP	141
3.2.5	System Management	142
3.2.5.1	TR-069.....	142
3.2.5.2	SNMP.....	143
3.2.5.3	Telnet with CLI	145
3.2.5.4	UPnP.....	146
3.3	APPLICATIONS	146
3.3.1	Mobile Application	147
3.3.1.1	SMS	147
3.3.1.2	USSD.....	149
3.3.1.3	Network Scan.....	150
3.3.1.4	Remote Management.....	151
3.3.2	Captive Portal.....	154
3.3.2.1	Captive Portal Configuration	154
3.4	SYSTEM	156
3.4.1	System Related	156
3.4.1.1	Change Password.....	156
3.4.1.2	System Information	157
3.4.1.3	System Status.....	157
3.4.1.4	System Tools	158
3.4.2	Scheduling.....	162
3.4.3	External Servers.....	163
3.4.3.1	External Server List.....	164
3.4.3.2	External Server Configuration	164
3.4.4	MMI.....	165
3.4.4.1	Web UI	165

ADDITIONAL INFORMATION ERROR! BOOKMARK NOT DEFINED.

Chapter 1 Introduction

Thank you for purchasing the Proroute GEM420 4G Cellular M2M Gateway. For M2M (Machine-to-Machine) applications, the Proroute Cellular M2M Gateway is absolutely the right choice. With built-in world-class 4G LTE module, you just need to insert SIM card from local mobile carrier to get to Internet. The redundant SIM design provides a more reliable WAN connection for critical applications. By VPN tunneling technology, remote sites easily become a part of Intranet, and all data are transmitted in a secure (256-bit AES encryption) link. To meet a variety of M2M application requirements, Proroute Cellular M2M Gateway products are based on modular design. A new functional module can replace current one to support new application in short time, such as for NFC or GPS applications.

This GEM420 series product is loaded with essential security features including VPN, firewall, NAT, port forwarding, DHCP server and many other powerful features for complex and demanding business and M2M (Machine-to-Machine) applications. The redundancy design in fallback 9-48 VDC power terminal, dual SIM cards and VRRP function makes the device as a back-up in power, network connection and data transmission without lost.

Main Features:

- Provide various and configurable WAN connection.
- Support dual SIMs for the redundant wireless WAN connection.
- Provide Ethernet ports for comprehensive LAN connection.
- Feature with VPN and NAT firewall to have powerful security.
- Support the robust remote or local management to monitor network.
- Designed by solid and easy-to-mount metal body for business and M2M environment to work with a variety M2M (Machine-to-Machine) applications.

Before you install and use this product, please read this manual in detail for fully exploiting the functions of this product.

1.1 Contents List

Items	Description	Contents	Quantity
1	GEM420AM Cellular M2M Gateway		1pcs
2	Cellular Antenna		2pcs
3	WiFi Antenna		2pcs
4	Power Adapter (DC 12V/2A)		1pcs
5	DC Jack Converter		1pcs
6	RJ45 Cable		1pcs
7	Console Cable		1pcs
8	CD (Manual)		1pcs
9	Wall Mount Kits		2pcs
10	DIN-Rail Bracket		1pcs

1.2 Hardware Installation

1.2.1 WARNING



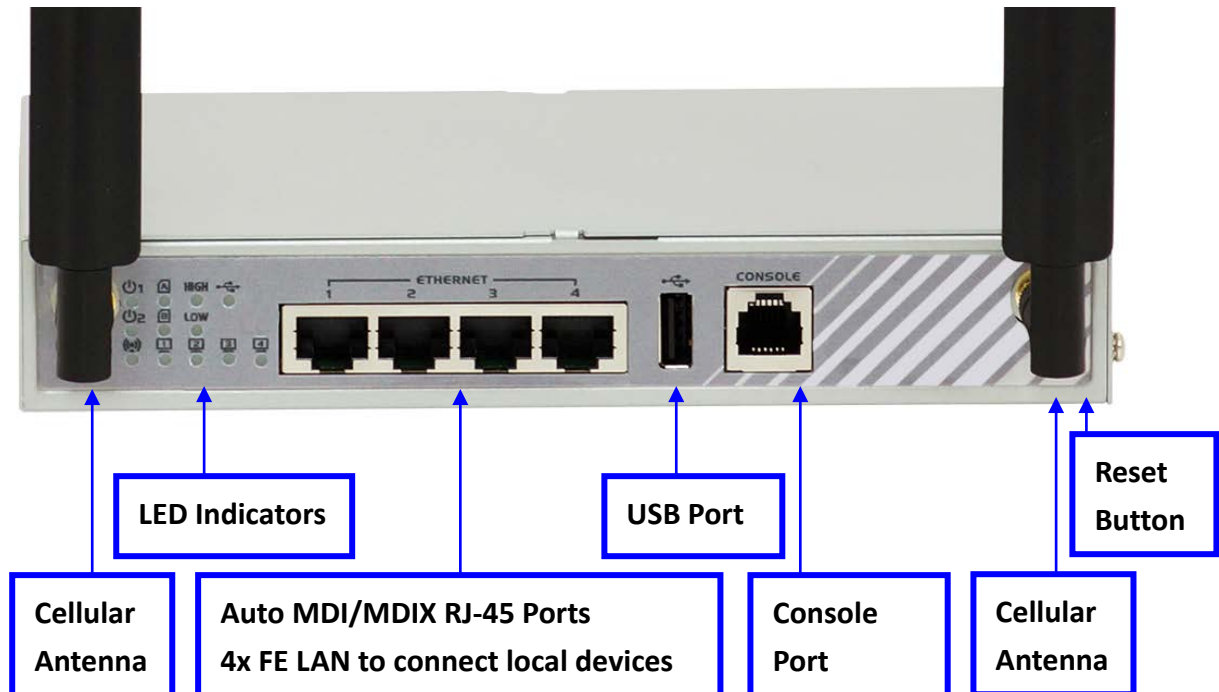
Attention

- Do not use the product in high humidity or high temperatures.
- Only use the power adapter that comes with the package. Using a different voltage rating power adaptor is dangerous and may damage the product.
- Do not open or repair the case yourself. If the product is too hot, turn off the power immediately and have it repaired at a qualified service center.
- Place the product on a stable surface and avoid using this product and all accessories outdoors.

1.2.2 SYSTEM REQUIREMENTS

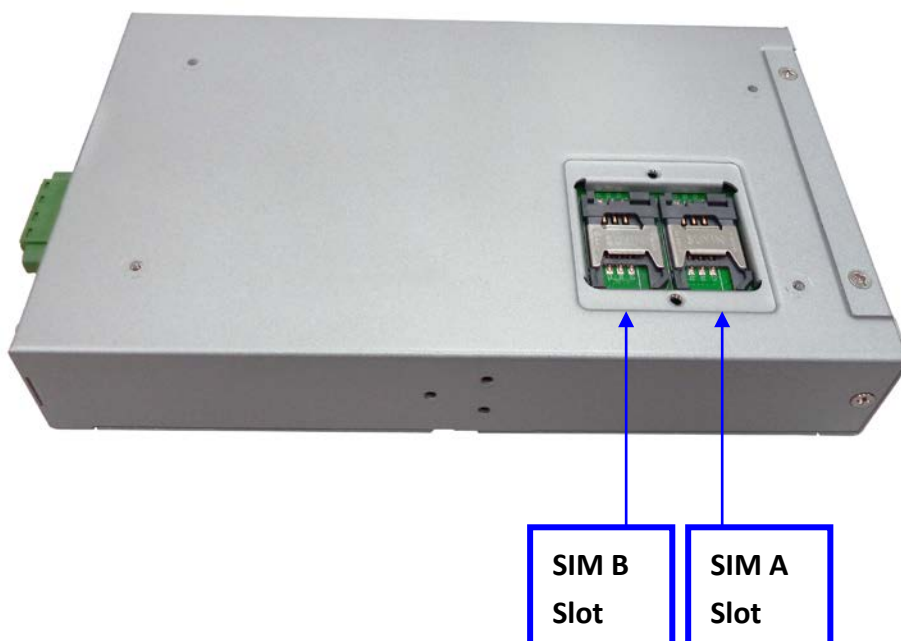
Network Requirements	• An Ethernet RJ-45 cable or DSL modem • 3G or LTE cellular service subscription • IEEE 802.11n or 802.11b/g wireless clients • 10/100 Ethernet adapter on PC
Web-based Configuration Utility Requirements	Computer with the following: • Windows®, Macintosh, or Linux-based operating system • An installed Ethernet adapter Browser Requirements: • Internet Explorer 6.0 or higher • Chrome 2.0 or higher • Firefox 3.0 or higher • Safari 3.0 or higher

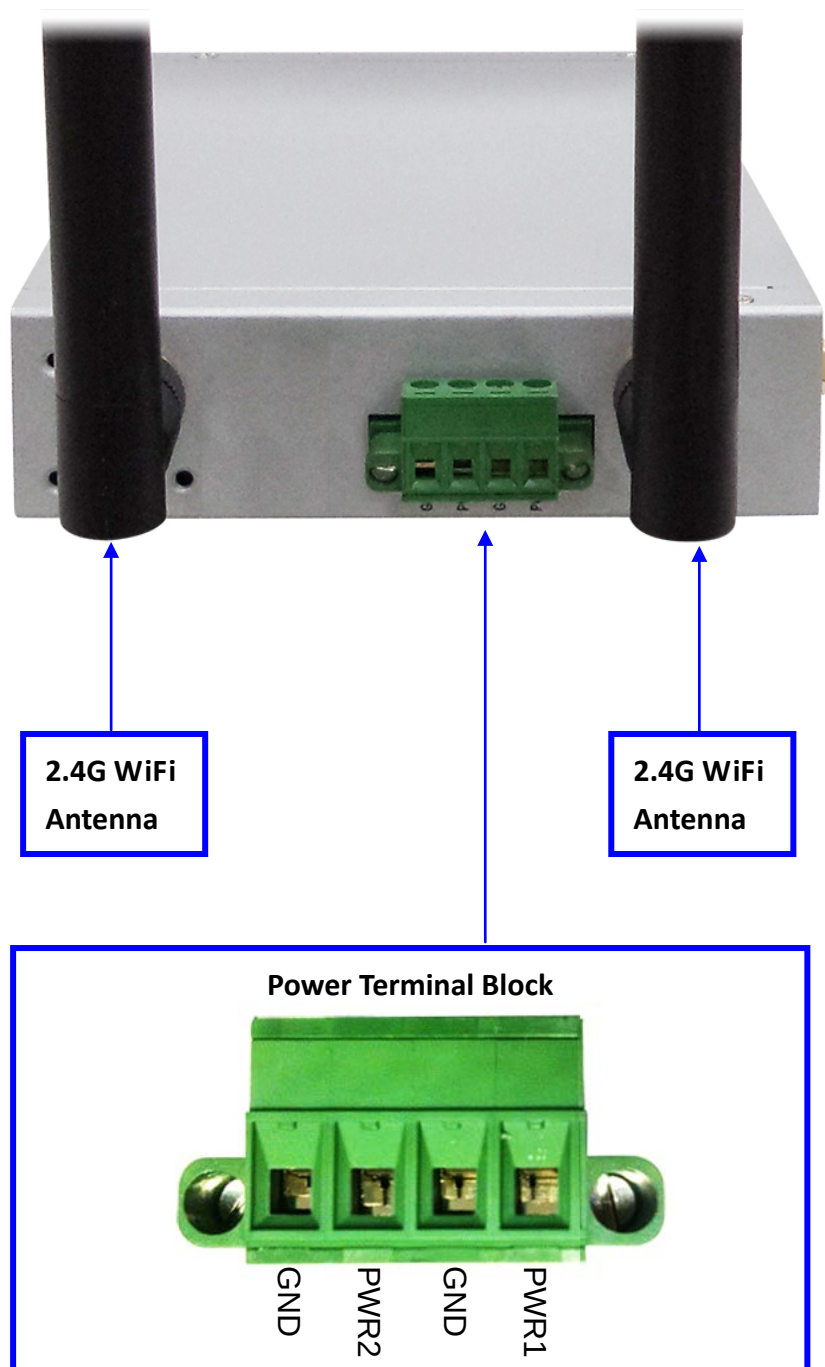
1.2.3 Hardware Configuration



✖Reset Button

The RESET button provides user with a quick and easy way to resort the default setting. Press the RESET button continuously for 6 seconds, and then release it. The device will restore to factory default settings.





1.2.4 LED Indication



LED Icon	Indication	LED Color	Description
	Power Source 1	Green	Steady ON: Device is powered on by power source 1
	Power Source 2 (* ¹)	Green	Steady ON: Device is powered on by power source 2
	WLAN (WiFi)	Green	Steady ON: Wireless radio is enabled Flash: Data packets are transferred OFF: Wireless radio is disabled
	SIM A (* ²)	Green	Steady ON: SIM card A is chosen for connection
	SIM B	Green	Steady ON: SIM card B is chosen for connection
	LAN 1 ~ LAN 4	Green	Steady ON: Ethernet connection of LAN is established Flash: Data packets are transferred
	High Cellular Signal	Green	Steady ON: The signal strength of Cellular is strong
	Low Cellular Signal	Green	Steady ON: The signal strength of Cellular is weak
	USB	Green	Steady ON: If USB 3G dongle is attached

- 1 If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. The LED of power source 2 will remain OFF at this condition.
- 2 The SIM LED indicates which SIM socket will be chosen for connection by system setting, no matter SIM card is inserted or not.

Chapter 2 Getting Started

This chapter describes how to install and configure the hardware and how to use the setup wizard to configure the network with the web GUI of GEM420 series.

2.1 Hardware Installation

2.1.1 Mount the Unit

The GEM420 series can be placed on a desktop, mounted on the wall, or mounted on a DIN-rail. It has designed with “ears” for attaching to the wall or the inside of a cabinet. The wall-mount kits and DIN-rail bracket are not screwed on the product when out of factory. Please screw the wall-mount kits and DIN-rail bracket on the product first.

2.1.2 Insert the SIM Card

WARNING: BEFORE INSERTING OR CHANGING THE SIM CARD, PLEASE MAKE SURE THAT POWER OF THE DEVICE IS SWITCHED OFF.

The SIM card slots are located at the bottom side of GEM420 housing in order to protect the SIM card. You need to unscrew and remove the outer SIM card cover before installing or removing the SIM card. Please follow the instructions to insert a SIM card. After SIM card is well placed, screw back the outer SIM card cover.

Step 1:

Follow red arrow to unlock SIM socket

Step 2:

Lift up SIM holder, and insert SIM card

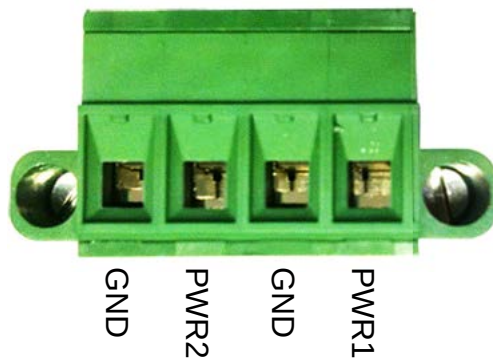
Step 3:

Put back SIM holder, and follow red arrow to lock SIM socket



2.1.3 Connecting Power

The GEM420 series can be powered by connecting a power source to the terminal block. **It supports dual 9 to 48VDC power inputs**³. Following picture is the power terminal block pin assignments. Please check carefully and connect to the right power requirements and polarity.



There are a DC converter and a DC12V/2A power adapter in the package for you to easily connect DC power adapter to this terminal block.



2.1.4 Connecting to the Network or a Host

The GEM420 series provides four RJ-45 ports to connect 10/100Mbps Ethernet. It can

³ If both of power source 1 and power source 2 are connected, the device will choose power source 1 first. If power outage occurred from power source 1, this device will switch to power source 2 automatically and seamlessly.

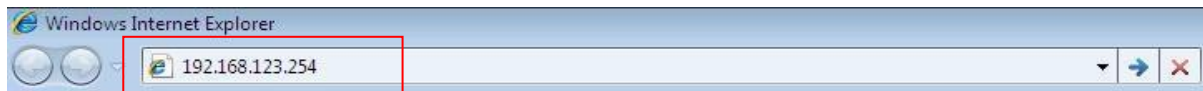
auto detect the transmission speed on the network and configure itself automatically. Connect the Ethernet cable to the RJ-45 ports of the device. Plug one end of an Ethernet cable into your computer's network port and the other end into one of GEM420 series for LAN ports on the front panel. If you need to configure or troubleshoot the device, you may need to connect the GEM420 series directly to the host PC. In this way, you can also use the RJ-45 Ethernet cable to connect the GEM420 series to the host PC's Ethernet port.

2.2 Easy Setup by Configuring WEB UI

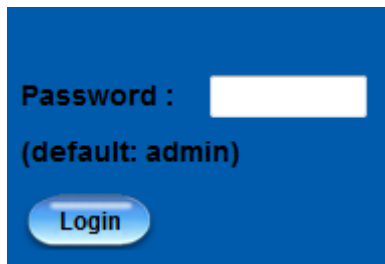
You can browse web UI to configure the device. First you need to launch the Setup Wizard browser and then the Setup Wizard will guide you step-by-step to finish the setup process.

Browse and Activate the Setup Wizard

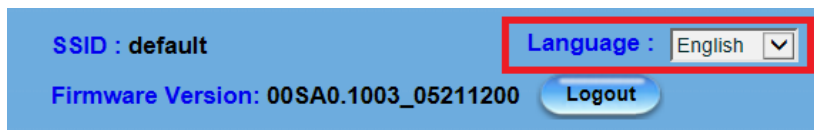
Type in the IP Address (<http://192.168.123.254>)⁴



When you see the login page, type the password 'admin'⁵ and then click '**login**' button.



After login, select your **language** from the list.

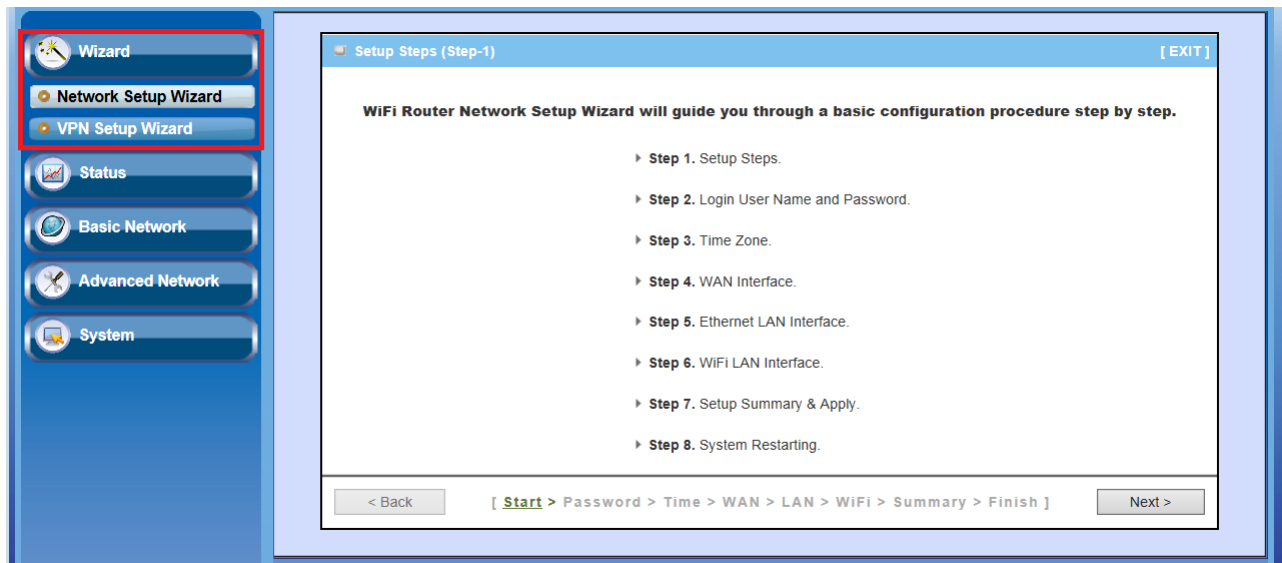


2.2.1 Wizard

Select "**Wizard**" for basic network settings and VPN settings in a simple way. Or, you can go to **Basic Network / Advanced Network / System** to setup the configuration by your own selection.

⁴ The default LAN IP address of this gateway is 192.168.123.254. If you change it, you need to type new IP address.

⁵ It's strongly recommending you to change this login password from default value.

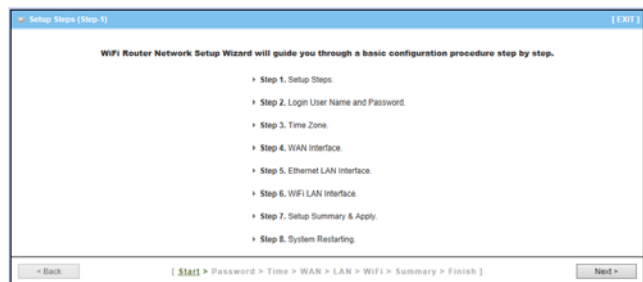


A. Configure with the Network Setup Wizard

Step 1

The network setup wizard will guide you to finish some basic settings, including login password, time zone, WAN interface, Ethernet LAN interface and WiFi LAN interface.

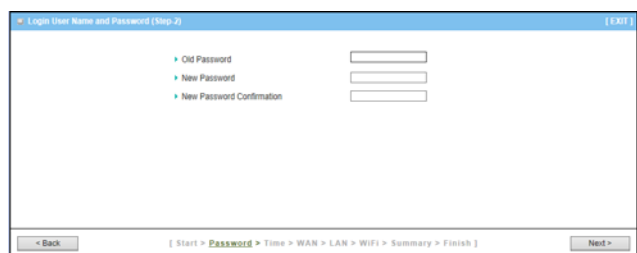
Press “**Next**” to start the wizard.



Step 2: Change Password

Password Configuration: You can change the login password of Web UI here. It's strongly recommending you to change this login password from default value.

Press “**Next**” to continue.



Step 3: Time Zone

Time Zone Configuration: It will detect your time zone automatically. If the result of auto detection is not correct, you can press “Detect Again” button or select manually.



Press “**Next**” to continue.

Step 4: WAN

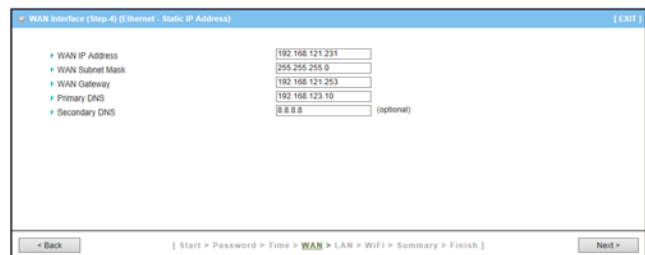
WAN Interface Configuration: Choose type of WAN connection. You can select Ethernet WAN if you want to connect to Internet through fixed line. Or select 3G/4G if you want to connect to Internet through 3G/4G network. A variety of WAN types are available for Ethernet WAN connection.



Press “**Next**” to continue.

Step 4-1: Ethernet (Static IP Address)

If choosing Ethernet->Static IP Address, you need to input all IP address that you get from ISP (Internet Service Provider) manually. This option is usually chosen when you get a fixed IP address from ISP.



Press “**Next**” to continue.

Step 4-2: Ethernet (Dynamic IP Address)

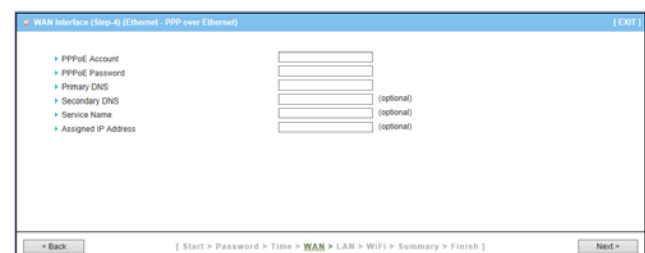
If choosing Ethernet->Dynamic IP Address, you can input host name or registered MAC address when your ISP requests it. In most cases, you can leave them as blank and go next. This option is usually chosen when you get a dynamic IP address from ISP.



Press “**Next**” to continue.

Step 4-3: Ethernet (PPPoE)

If choosing Ethernet->PPP over Ethernet (so-called PPPoE), you need to input account and password that you get from ISP. For other fields, you can leave them as blank in most cases. This option is



usually chosen when you use ADSL for WAN connection.

Press **“Next”** to continue.

Step 4-4: Ethernet (PPTP)

If choosing Ethernet->PPTP, you need to input required dial-up information that you get from ISP. This option is usually chosen when your ISP requests it.

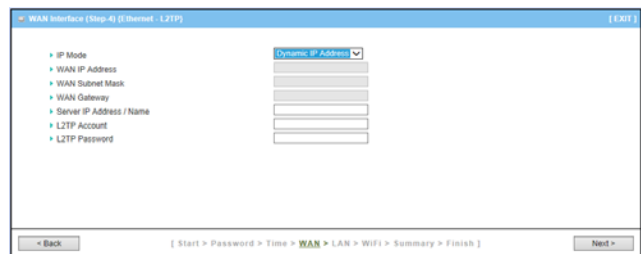
Press **“Next”** to continue.



Step 4-5: Ethernet (L2TP)

If choosing Ethernet->L2TP, you need to input required dial-up information that you get from ISP. This option is usually chosen when your ISP requests it.

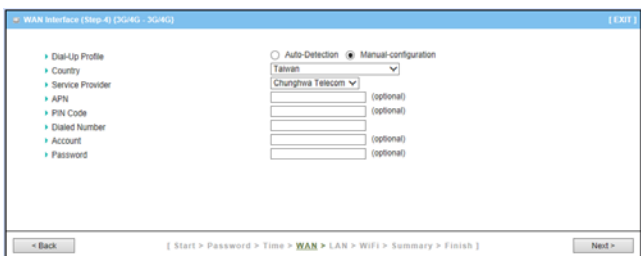
Press **“Next”** to continue.



Step 4-6: 3G/4G

If choosing 3G/4G->3G/4G, please make sure you have inserted SIM card. If not, please power off this gateway, and insert SIM card first. Then you can select “Auto-Detection” to finish dial-up profile automatically. This option is chosen when you want to connect to Internet through 3G/4G network instead of fixed line broadband.

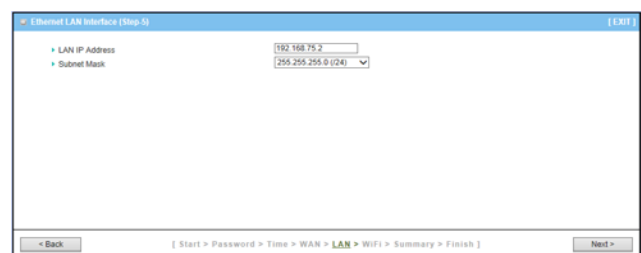
Press **“Next”** to continue.



Step 5: Ethernet LAN

LAN Interface Configuration: Change the LAN IP address and subnet mask of this gateway. You can keep the default setting and go to next step.

Press **“Next”** to continue.



Step 6: WiFi LAN

WiFi LAN Interface Configuration:

Change the SSID, Channel Number, Authentication and Encryption Algorithm for first virtual AP of this gateway. You will see on your PC when doing wireless network scan. It's strongly recommending you to add authentication and encryption in your wireless network to prevent any unknown WiFi clients and keep transferred data secured. You can also keep the default setting and go to next step.

Press **"Next"** to continue.



WiFi LAN Interface (Step-6) (2/4G) [EXIT]

- WiFi Module: ☒ Enable
- Network ID(SSID): JP 75
- Channel: Auto
- Authentication: Auto
- Encryption: None

[< Back] [Start > Password > Time > WAN > LAN > **WiFi** > Summary > Finish] [Next >]

Step 7: Confirm and Apply

Check the new settings again. If all information is correct, please press "Apply" button to save new settings. Then it will take 65 seconds to restart this gateway and take new settings effective.



WiFi Router Network Setup Summary & Apply (Step-7) [EXIT]

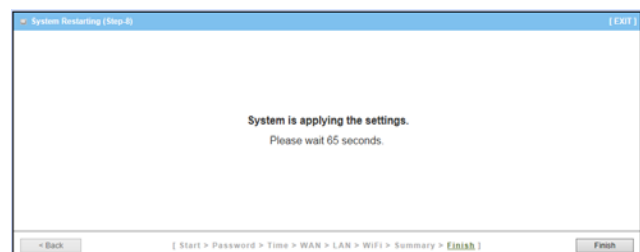
Please confirm the information below.

[WAN Settings]	
WAN Interface	Ethernet
WAN Type	Static IP Address
WAN IP Address	192.168.121.231
WAN Subnet Mask	255.255.255.0
WAN Gateway	192.168.121.253
Primary DNS	192.168.123.10
Secondary DNS	8.8.8.8
[Ethernet LAN Settings]	
IP Address	192.168.75.2
Subnet Mask	255.255.255.0
[WiFi LAN 2.4G Settings]	
WiFi Module	Enable
SSID	JP 75
Channel	Auto
Authentication	Auto
Encryption	None

[Cancel] [Start > Password > Time > WAN > LAN > WiFi > **Summary** > Finish] [Apply]

Step 8: Counting Down

Configuration is completed. Press "Finish" button to close Setup Wizard and browser counts down for 65 seconds and provides you with "Click here" button to reconnect to the device.



System Restarting (Step-8) [EXIT]

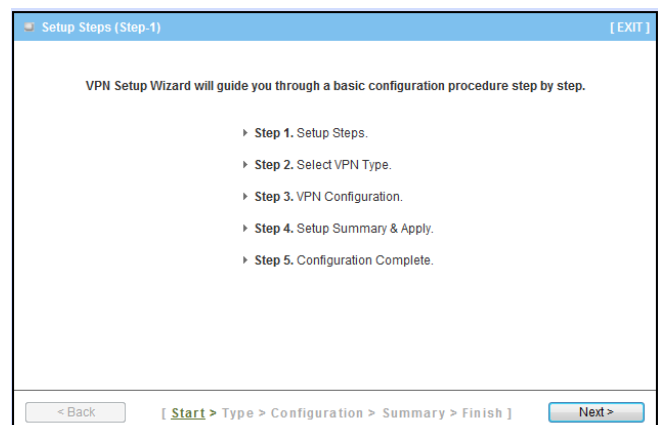
System is applying the settings.
Please wait 65 seconds.

[< Back] [Start > Password > Time > WAN > LAN > WiFi > Summary > **Finish**] [Finish]

B. Configure with the VPN Setup Wizard**Step 1**

The VPN setup wizard will guide you to finish profiles of IPSec, PPTP, and L2TP VPN connection quickly.

Press **"Next"** to start the wizard.



Setup Steps (Step-1) [EXIT]

VPN Setup Wizard will guide you through a basic configuration procedure step by step.

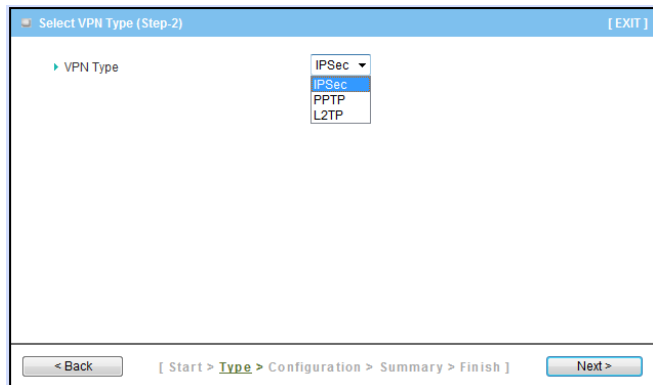
- ▶ Step 1. Setup Steps.
- ▶ Step 2. Select VPN Type.
- ▶ Step 3. VPN Configuration.
- ▶ Step 4. Setup Summary & Apply.
- ▶ Step 5. Configuration Complete.

[< Back] [**Start** > Type > Configuration > Summary > Finish] [Next >]

Step 2: VPN Type

Select type of VPN connection you want to create. Here you can choose IPSec, PPTP, or L2TP.

Press “**Next**” to continue.



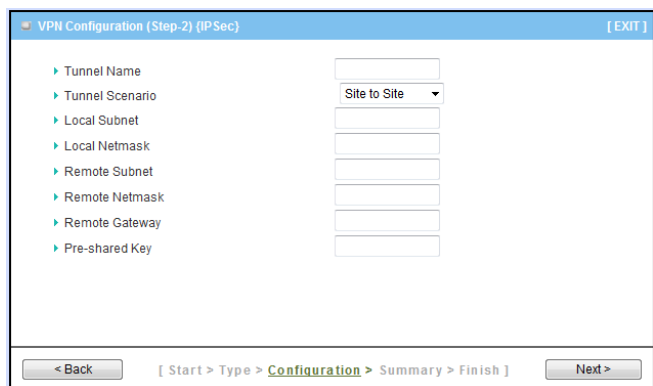
The screenshot shows the 'Select VPN Type (Step-2)' configuration window. It has a title bar with '[EXIT]' on the right. The main area contains a 'VPN Type' label and a dropdown menu with 'IPSec' selected, and 'PPTP' and 'L2TP' as other options. At the bottom, there is a navigation bar with '< Back', '[Start > Type > Configuration > Summary > Finish]', and 'Next >' buttons.

Step 2-1: IPSec

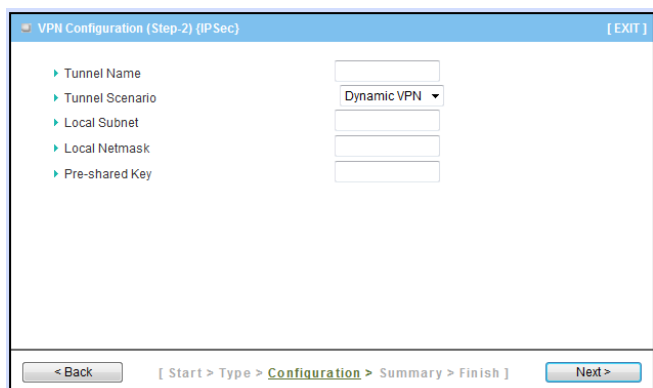
If choosing IPSec, there are two options of tunnel scenario can be chosen. “Site to Site” is for two offices to create VPN tunnel. “Dynamic VPN” is for remote users to connect to office. For other options, please go to Advanced Network->VPN to setup. Input the required network information and pre-shared key for VPN connection.

For Dynamic VPN, you don’t need to input network information of remote subnet and remote gateway.

Press “**Next**” to continue.



The screenshot shows the 'VPN Configuration (Step-2) (IPSec)' window with the 'Tunnel Scenario' set to 'Site to Site'. It includes fields for Tunnel Name, Local Subnet, Local Netmask, Remote Subnet, Remote Netmask, Remote Gateway, and Pre-shared Key. The bottom navigation bar shows '[Start > Type > Configuration > Summary > Finish]' with 'Configuration' highlighted.

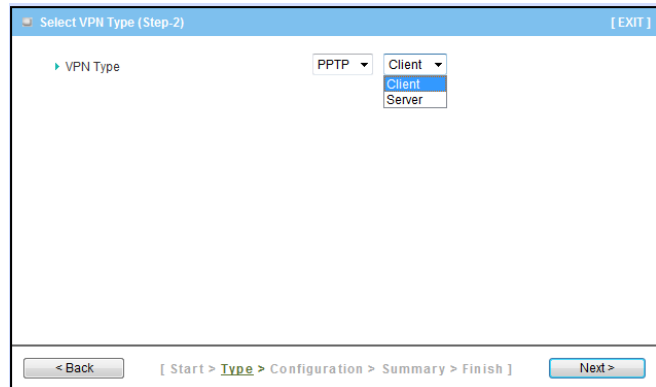


The screenshot shows the 'VPN Configuration (Step-2) (IPSec)' window with the 'Tunnel Scenario' set to 'Dynamic VPN'. It includes fields for Tunnel Name, Local Subnet, Local Netmask, and Pre-shared Key. The bottom navigation bar shows '[Start > Type > Configuration > Summary > Finish]' with 'Configuration' highlighted.

Step 2-2: PPTP

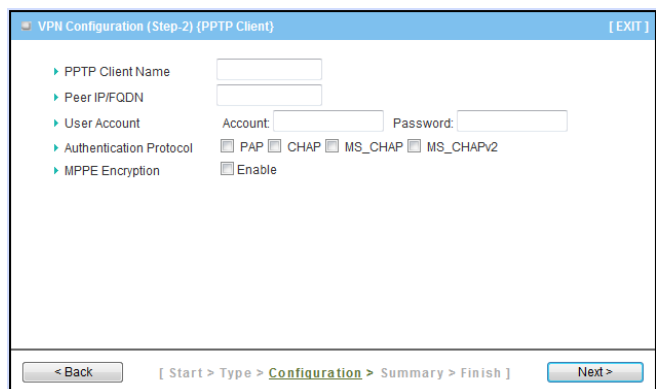
If choosing PPTP, there are two options of mode can be chosen. Choose “Client” if you want this device to connect to another PPTP server. Or choose “Server” if you want other PPTP clients to connect to it.

Press “**Next**” to continue.



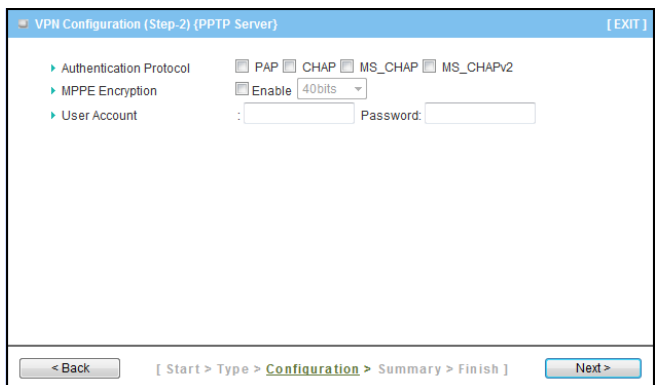
If choosing PPTP Client, please input tunnel name, IP/FQDN of PPTP server, username/password, authentication, and MPPE options. Please make sure these settings are accepted by PPTP server. Otherwise, remote PPTP server will reject the connection.

Press “**Next**” to continue.



If choosing PPTP Server, please select options of authentication and MPPE. You also need to create a set of username and password for PPTP clients. In this wizard, you can only create one user account. If you want to create more user accounts, please go to Advanced Network->VPN-> PPTP to add more users.

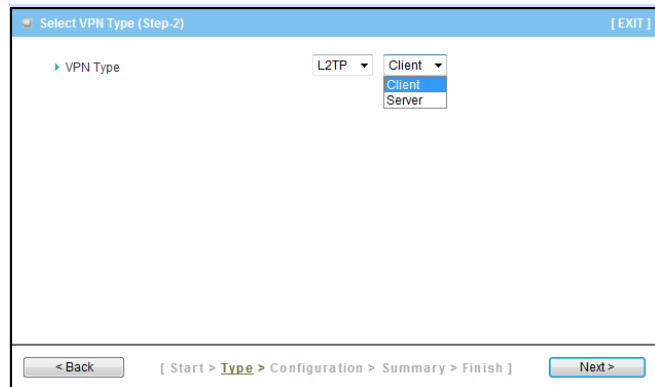
Press “**Next**” to continue.



Step 2-3: L2TP

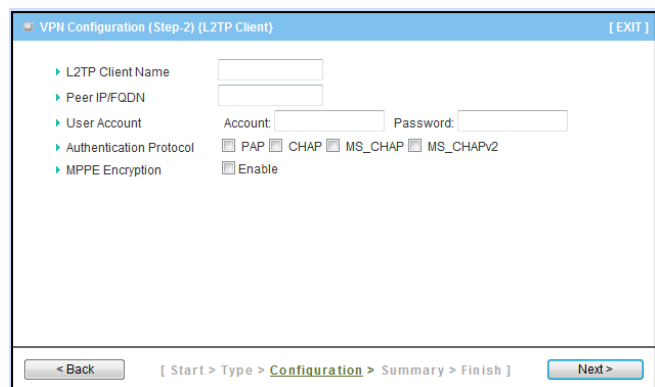
If choosing L2TP, there are two options of mode can be chosen. Choose “Client” if you want this device to connect to another L2TP server. Or choose “Server” if you want other L2TP clients to connect to it.

Press “**Next**” to continue.



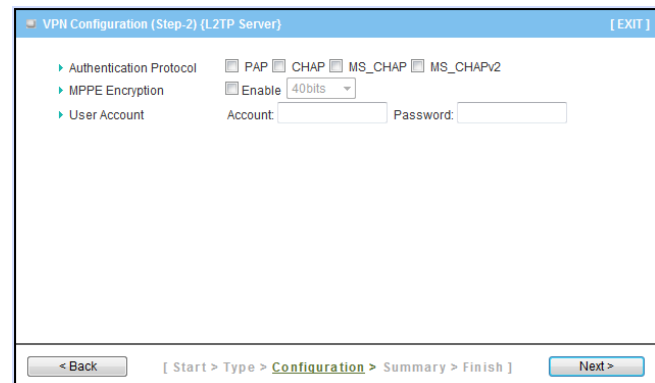
If choosing L2TP Client, please input tunnel name, IP/FQDN of L2TP server, username/password, authentication, and MPPE options. Please make sure these settings are accepted by L2TP server. Otherwise, remote L2TP server will reject the connection.

Press “**Next**” to continue.



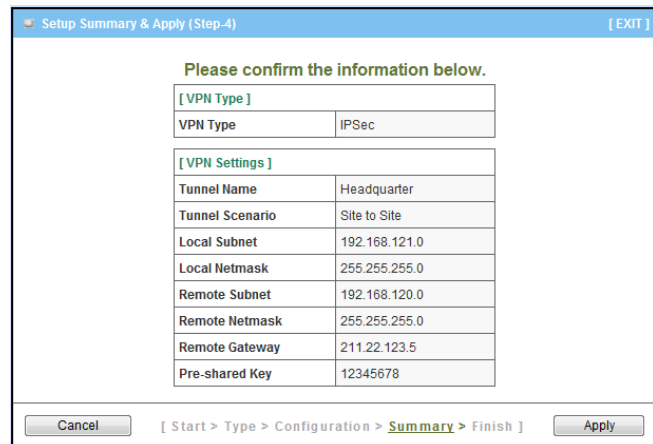
If choosing L2TP Server, please select options of authentication and MPPE. You also need to create a set of username and password for L2TP clients. In this wizard, you can only create one user account. If you want to create more user accounts, please go to Advanced Network->VPN-> L2TP to add more users.

Press “**Next**” to continue.



Step 3: Confirm and Apply

Confirm new settings. If all new settings are correct, please press “Apply” button to save these new settings and take them effective.



Setup Summary & Apply (Step-4) [EXIT]

Please confirm the information below.

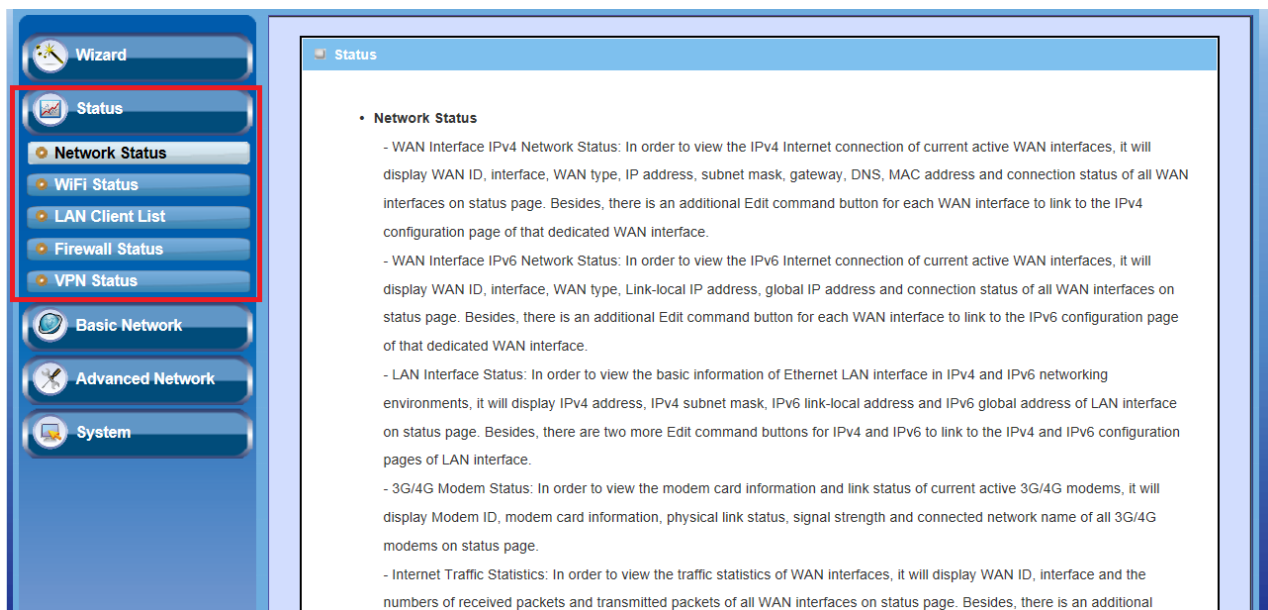
[VPN Type]	
VPN Type	IPSec

[VPN Settings]	
Tunnel Name	Headquarter
Tunnel Scenario	Site to Site
Local Subnet	192.168.121.0
Local Netmask	255.255.255.0
Remote Subnet	192.168.120.0
Remote Netmask	255.255.255.0
Remote Gateway	211.22.123.5
Pre-shared Key	12345678

Cancel [Start > Type > Configuration > Summary > Finish] Apply

2.2.2 Status

There are 5 kinds of system status to be shown at this window. They are Network Status, WiFi Status, LAN Client List, Firewall Status and VPN Status.



The screenshot shows the 'Status' window in the router's web interface. On the left sidebar, the 'Status' menu is highlighted with a red box, and its sub-items are listed: Network Status, WiFi Status, LAN Client List, Firewall Status, and VPN Status. The main content area displays the 'Network Status' section, which includes detailed information about WAN and LAN interfaces, 3G/4G modem status, and internet traffic statistics.

• Network Status

- WAN Interface IPv4 Network Status: In order to view the IPv4 Internet connection of current active WAN interfaces, it will display WAN ID, interface, WAN type, IP address, subnet mask, gateway, DNS, MAC address and connection status of all WAN interfaces on status page. Besides, there is an additional Edit command button for each WAN interface to link to the IPv4 configuration page of that dedicated WAN interface.
- WAN Interface IPv6 Network Status: In order to view the IPv6 Internet connection of current active WAN interfaces, it will display WAN ID, interface, WAN type, Link-local IP address, global IP address and connection status of all WAN interfaces on status page. Besides, there is an additional Edit command button for each WAN interface to link to the IPv6 configuration page of that dedicated WAN interface.
- LAN Interface Status: In order to view the basic information of Ethernet LAN interface in IPv4 and IPv6 networking environments, it will display IPv4 address, IPv4 subnet mask, IPv6 link-local address and IPv6 global address of LAN interface on status page. Besides, there are two more Edit command buttons for IPv4 and IPv6 to link to the IPv4 and IPv6 configuration pages of LAN interface.
- 3G/4G Modem Status: In order to view the modem card information and link status of current active 3G/4G modems, it will display Modem ID, modem card information, physical link status, signal strength and connected network name of all 3G/4G modems on status page.
- Internet Traffic Statistics: In order to view the traffic statistics of WAN interfaces, it will display WAN ID, interface and the numbers of received packets and transmitted packets of all WAN interfaces on status page. Besides, there is an additional

A. Network Status

In Network Status page, you can review lots information of network status, including a connection diagram, WAN IPv4 status, WAN IPv6 status, LAN status, and 3G/4G modem status. You can also check the device time at the bottom of this page.

Connection Diagram



1. **3G/4G Icon:** Indicates if 3G/4G connection is established or not.
2. **xDSL/Cable Icon:** Indicates if Ethernet WAN connection is established or not.
3. **Wired Client Icon:** Indicates how many Ethernet clients are connected now.
4. **WiFi Client Icon:** Indicates how many WiFi clients are connected now.

WAN Interface IPv4 Network Status

Display WAN type, IPv4 information, MAC information, and connection status of multiple WAN interfaces in IPv4 networking. Press “Edit” button if you want to change settings.

WAN Interface IPv4 Network Status									
WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	Ethernet	Static IP	192.168.121.231	255.255.255.0	192.168.121.253	192.168.123.10, 8.8.8.8	00:50:18:96:63:52	N/A	Edit
WAN-2	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0		Disconnected	Edit
WAN-3	USB 3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0		Disconnected	Edit

WAN Interface IPv6 Network Status

Display WAN type, IPv6 information, and connection status of multiple WAN interfaces in IPv6 networking. Press “Edit” button if you want to change settings.

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1	Disable					Edit

LAN Interface Status

Display IPv4 and IPv6 information of local network. Press “Edit” button if you want to change settings.

LAN Interface Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
192.168.75.2	255.255.255.0		/64	Edit IPv4 Edit IPv6

3G/4G Modem Status

Display modem information, link status, signal strength, and network (carrier) name of 3G/4G connection.

3G/4G Modem Status Refresh					
Modem ID	Card Information	Link Status	Signal Strength	Network Name	Actions
3G-1	D18Q1	Disconnected	N/A	N/A	Detail
3G-2	N/A	Disconnected	N/A	N/A	Detail

Press “Detail” button to browse detailed information of cellular connection status.

Modem Information				
Physical Interface	Module Name	IMEI/MEID	HW Version	FW Version
3G1	D18Q1	356318040749638	20002	D18Q1_v10.10.1 [Jun 27 2014 11:00:00]

SIM Status			
SIM	PIN Code Status	PIN Code Remaining Times	PUK Code Remaining Times
N/A	SIM card not insert	0	0

Service Information									
Operator	Cell Broadcast	MCC	MNC	LAC	TAC	Cell ID	Service Type	Band	RSSI
CS Register Status	EcIo	PS Register Status	PS Attached Status	Roaming Status	IMSI	SMSC	MSISDN		
Unregistered		Unregistered	Detached	Not Roaming					

Internet Traffic Statistics

Display number of transmitted packets and received packets of each WAN interface.

Internet Traffic Statistics			
WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0
WAN-2		0	0
WAN-3		0	0

Device Time

Display current time information of device.

Device Time: Thu, 26 Jun 2014 14:25:15 +0800

B. WiFi Status

WiFi Virtual AP List: In order to view the basic information of WiFi virtual APs, it will display operation band, virtual AP ID, WiFi activity, operation mode, SSID, channel, WiFi system, WiFi security approach and MAC address of all virtual APs on status page. Besides, there is an additional Edit command button for each virtual AP to link to the configuration page

of that dedicated virtual AP.

WiFi Virtual AP List									
Op. Band	VAP ID	WiFi Enable	Op. Mode	SSID	Channel	WiFi System	Auth.& Security	MAC Address	Action
2.4G	VAP-1	☒	AP Router	JP.75	Auto	B/G/N Mixed	Auto(None)	00:50:18:96:63:53	Edit
2.4G	VAP-2	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	02:50:18:96:63:53	Edit
2.4G	VAP-3	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	06:50:18:96:63:53	Edit
2.4G	VAP-4	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	0A:50:18:96:63:53	Edit
2.4G	VAP-5	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	0E:50:18:96:63:53	Edit
2.4G	VAP-6	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	12:50:18:96:63:53	Edit
2.4G	VAP-7	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	16:50:18:96:63:53	Edit
2.4G	VAP-8	☐	AP Router	default	Auto	B/G/N Mixed	Auto(None)	1A:50:18:96:63:53	Edit

WiFi Traffic Statistics: In order to view the traffic statistics of WiFi virtual APs, it will display operation band, virtual AP ID and the numbers of received packets and transmitted packets of all virtual APs on status page. Besides, there is an additional Reset command button for each virtual AP to clear the traffic statistics.

WiFi Traffic Statistics					Refresh
Op. Band	VAP ID	Received Packets	Transmitted Packets	Action	
2.4G	VAP-1	0	0	Reset	
2.4G	VAP-2	0	0	Reset	
2.4G	VAP-3	0	0	Reset	
2.4G	VAP-4	0	0	Reset	
2.4G	VAP-5	0	0	Reset	
2.4G	VAP-6	0	0	Reset	
2.4G	VAP-7	0	0	Reset	
2.4G	VAP-8	0	0	Reset	

C. LAN Client List

In order to view the connection of current active wired/wireless clients, it will display LAN interface, IP address configuration, host name, MAC address and remaining lease time of all client devices on status page.

LAN Client List				
LAN Interface	IP Address Configuration	Host Name	MAC Address	Remaining Lease Time
Ethernet	Dynamic / 192.168.75.100	amit-alpha	20-6A-6A-6A-6A-B6	21:14:10
WiFi	Dynamic / 192.168.75.101	amit-alpha	60-D8-19-26-90-BD	23:43:09
WiFi	Dynamic / 192.168.75.102	android-4bd032267756f548	00-37-6D-26-A2-1C	23:58:14

D. Firewall Status

In Firewall Status page, you can review lots information of filter status, including Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and other options of firewall.

Packet Filters

Display all detected contents of firing activated packet filter rules.

Packet Filters Edit [+]			
Activated Filter Rule	Detected Contents	IP	Time

URL Blocking

Display all blocked URLs of firing activated URL blocking rules.

URL Blocking Edit [+]			
Activated Blocking Rule	Blocked URL	IP	Time

Web Content Filters

Display all detected contents of firing activated Web content filter rules.

Web Content Filters Edit [+]			
Activated Filter Rule	Detected Contents	IP	Time

MAC Control

Display all blocked MAC addresses of firing activated MAC control rules.

MAC Control Edit [+]			
Activated Control Rule	Blocked MAC Addresses	IP	Time

Application Filters

Display all activated rules of application filters

Application Filters Edit [+]			
Filtered Application Category	Filtered Application Name	IP	Time

IPS

Display all activated rules of IPS.

IPS Edit [+]		
	Detected Intrusion	IP
		Time

Options

Display option settings of firewall.

Options Edit [+]			
Stealth Mode	SPI	Discard Ping from WAN	Remote Administrator Management

E. VPN Status

In VPN Status page, you can review lots information of VPN status, including IPsec status, PPTP Server status, PPTP Client status, L2TP Server status and L2TP Client status.

IPSec Status

Display the status of all activated tunnels of IPsec.

IPSec Status		Edit					
Tunnel Name	Tunnel Scenario	Local Subnet	Local Subnet Mask	Remote IP/FQDN	Remote Subnet	Remote Subnet Mask	Status

PPTP Server Status

Display the status of all activated accounts of PPTP server.

PPTP Server Status		Edit		
User Name	Peer IP/FQDN	Peer Virtual IP	Peer Call ID	Status

PPTP Client Status

Display the status of all activated PPTP clients.

PPTP Client Status		Edit			
PPTP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

L2TP Server Status

Display the status of all activated accounts of L2TP server.

L2TP Server Status		Edit		
User Name	Peer IP/FQDN	Virtual IP	Peer Call ID	Status

L2TP Client Status

Display the status of all activated L2TP clients.

L2TP Client Status		Edit			
L2TP Client Name	Interface	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status

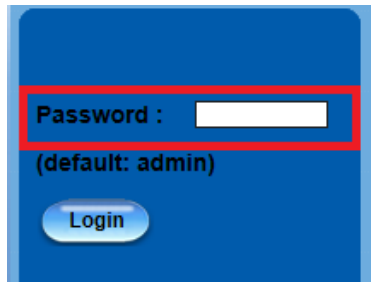
Chapter 3 Making Configurations

Whenever you want to configure your network or this device, you can access the Configuration Menu by opening the web browser and typing in the IP Address of the device. The default IP Address is: **192.168.123.254**. In the configuration section you may want to check the connection status of the device, to do Basic or Advanced Network setup

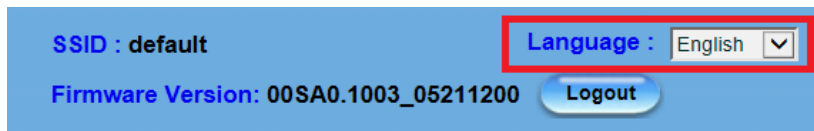
or to check the system status. These task buttons can be easily found in the cover page of the UI (User Interface).



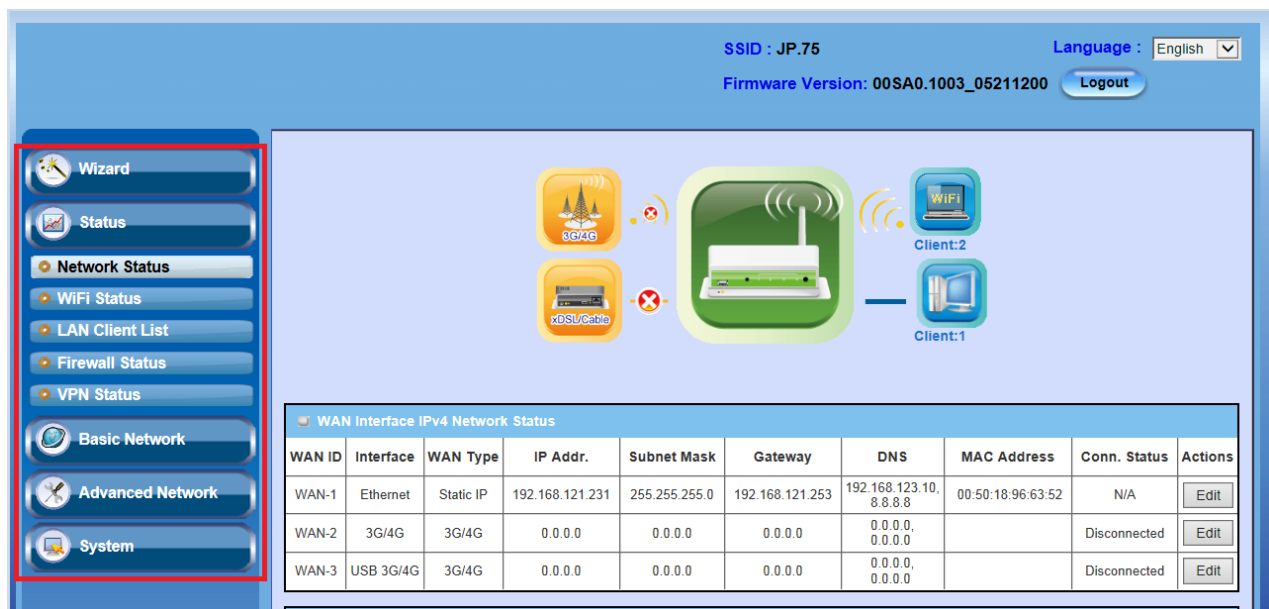
Enter the default password “**admin**” in the Password and then click ‘**Login**’ button.



After login, select your **language** from the list.



Afterwards, you can go **Wizard**, **Basic Network**, **Advanced Network** or **System** respectively on left hand side of web page.



Note: You can see the first screen is located at **Status >> Network Status** after you logged in and the screen shows the Network Connection Status below.

WAN Interface IPv4 Network Status									
WAN ID	Interface	WAN Type	IP Addr.	Subnet Mask	Gateway	DNS	MAC Address	Conn. Status	Actions
WAN-1	3G/4G	3G/4G	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0, 0.0.0.0	N/A	Disconnected	Edit
WAN-2		Disable							Edit
WAN-3		Disable							Edit

WAN Interface IPv6 Network Status						
WAN ID	Interface	WAN Type	Link-Local IP Address	Global IP Address	Connection Status	Actions
WAN-1		Disable				Edit

LAN Interface Status				
IPv4 Address	IPv4 Subnet Mask	IPv6 Link-Local Address	IPv6 Global Address	Actions
192.168.123.254	255.255.255.0		/64	Edit IPv4 Edit IPv6

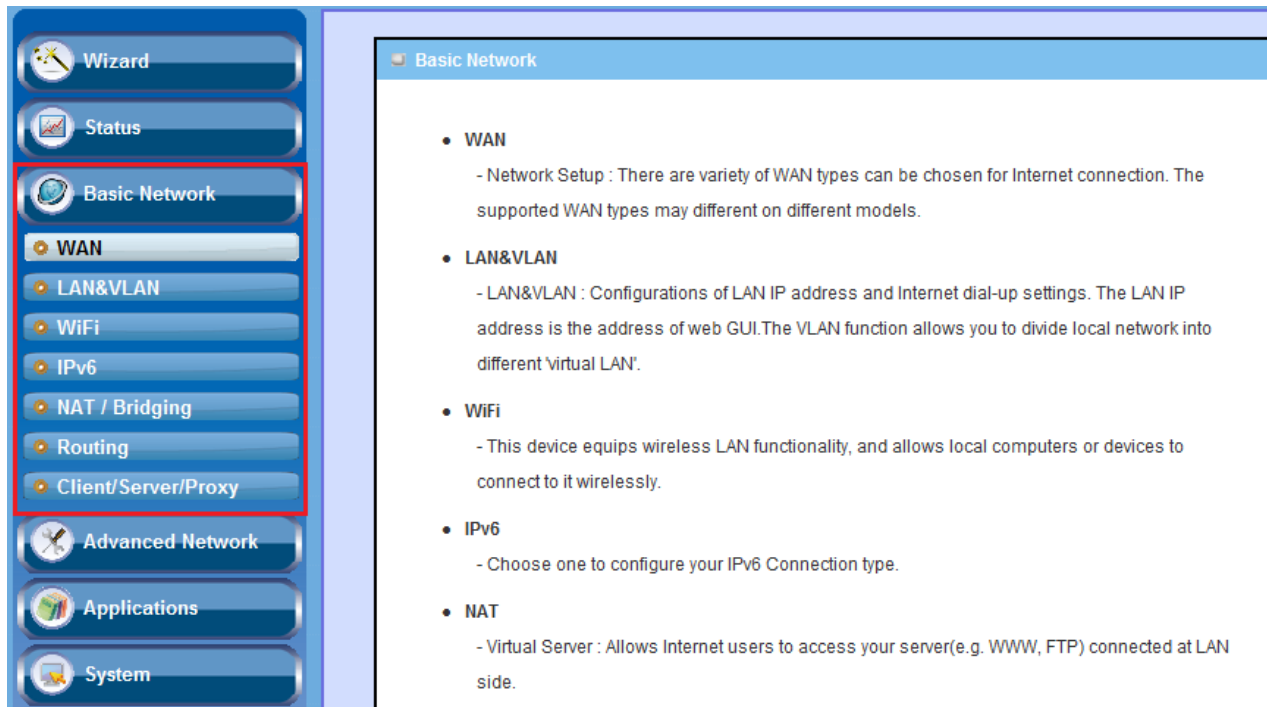
3G/4G Modem Status Refresh					
Modem ID	Card Information	Link Status	Signal Strength	Network Name	Actions
3G-1	D18Q1	Disconnected	N/A	N/A	Detail
3G-2	N/A	Disconnected	N/A	N/A	Detail

Internet Traffic Statistics			
WAN ID	Physical Interface	Received Packets	Transmitted Packets
WAN-1	3G/4G	0	0
WAN-2		0	0
WAN-3		0	0

You can check status of WiFi at **WiFi Status** page, connected clients at **LAN Client List** page, and other advanced function status at **Firewall Status** page and **VPN Status** page.

3.1 Basic Network

You can enter Basic Network for **WAN**, **LAN&VLAN**, **WiFi**, **IPv6**, **NAT/Bridging**, **Routing**, and **Client/Server/Proxy** settings as the icon shown here.



3.1.1 WAN Setup

This device is equipped with three WAN Interfaces to support different WAN types of connection. You can configure one by one to get proper Internet connection setup.

3G/4G WAN: The gateway has one 3G/4G⁶ modem built-in, please plug in SIM card and follow UI setting to setup.



Caution

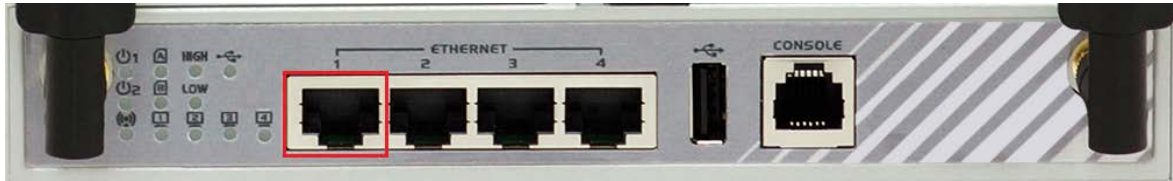
- Please **MUST POWER OFF** the gateway before you insert or remove SIM card.
- It will damage SIM card if you insert or remove SIM card during gateway is in operation.
- Please follow instructions at section 2.1.2.

USB 3G/4G WAN: The gateway has one USB port that can support USB 3G/4G modem dongle⁷. Please plug 3G/LTE USB dongle and follow UI setting to setup.

Ethernet WAN: The 1st Ethernet port can be configured as WAN connection. Please plug in RJ45 cable from your external DSL modem and follow UI setting to setup.

⁶ The specification of embedded module depends on respective model.

⁷ Please refer to compatibility (www.gem420.com) list to check which 3G or LTE dongles are supported by this device.



3.1.1.1 Physical Interface

Click on the **“Edit”** button for each WAN interface and you can get the detail physical interface settings and then configure the settings as well. By default, the WAN-1 interface is forced to **“Always-on”** mode, and operates as the primary internet connection; the interfaces WAN-2 and WAN-3 are disabled.

Physical Interface Internet Setup Load Balance				
Physical Interface List				
Interface Name	Physical Interface	Operation Mode	Line Speed	Action
WAN-1	Ethernet	Always on	0/0	Edit
WAN-2	-	Disable	0/0	Edit
WAN-3	-	Disable	0/0	Edit

1. **WAN-1:** The operation mode of this interface is forced to **“Always-on”** mode, and operates as the primary Internet connection. You can click on the respective **“Edit”** button and configure the rest items for this interface.
2. **WAN-2:** The operation mode of this interface is disabled by default, you can click on the respective **“Edit”** button to configure.
3. **WAN-3:** The operation mode of this interface is disabled by default, you can click on the respective **“Edit”** button to configure.

Interface Configuration (WAN- 1)	
Item	Setting
Physical Interface	Ethernet
Operation Mode	Always on
Line Speed	/ (Mbps)
VLAN Tagging	☐ Enable 2 (1-4095)

1. **Physical Interface:** Select the WAN interface from the available list. For this gateway, there are “Ethernet”, “3G/4G”, and “USB 3G/4G” items. If you want to

use embedded 3G/4G modem to operate as the primary Internet connection (WAN-1), please choose “3G/4G” for configuring the embedded 3G/4G modem as primary WAN connection. Or you can select “USB 3G/4G” if you want to use attached 3G/LTE USB dongle as an Internet connection. Otherwise, you can choose “Ethernet” if you would like the RJ45 port to be the primary Internet connection.

2. **Operation Mode:** There are three options for this item.

Always-on: Set this WAN interface to be active all the time. It means two or more Internet connections will be established simultaneously, and outgoing data will be transferred through these WAN connections base on load balance policies. This mode is especially suitable for high bandwidth requirement, such as video stream transmission.

Failover: Set this WAN interface to be a backup WAN connection. This WAN interface won't be active until other WAN connection is failed. If you specified a certain WAN interface as a “**Failover**” WAN, you have to further identify which WAN interface is to be failover and fallback. For some mission-critical applications, this gateway supports “Seamless failover”⁸ to shorten switch time between WAN interface failover and fallback.

▶ Operation Mode	Failover ▼	WAN-1 ▼	Seamless ☐ Enable
------------------	------------	---------	--

For the example above, if WAN-1 connection is broken, this gateway will try to failover the Internet connection to this WAN interface automatically. When WAN-1 connection becomes available again, the Internet connection will switch back to WAN-1 automatically.

Disable: Deactivate this WAN interface.

3. **Line Speed:** You can specify the upstream / downstream speed (Mbps) for the corresponding WAN connection. Such information will be referred in QoS and load balance function to manage the traffic load for each WAN connection.
4. **VLAN Tagging:** If your ISP required a VLAN tag been inserted into the WAN packets, you can enable this setting, and enter the specified tag value.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the

⁸ Please note your ISP will charge the connection fee even if it's set to seamless failover.

changes.

3.1.1.2 Internet Setup

There are three physical WAN interfaces that you can configure one by one to get proper Internet connection setup. They include the 3G/4G WAN, if the ISP is a mobile operator that can provide LTE, HSPA+, HSPA, WCDMA, EDGE, GPRS data services⁹. And the Ethernet WAN, if a fixed line ISP that provides xDSL or cable modem with Dynamic IP, Static IP, PPPoE, PPTP and L2TP connection types. In addition, for 3G/4G WAN, the device product supports Dual-SIM failover mechanism.

Hereafter are some details of WAN type options:

3G/4G: If you have subscribed 3G/LTE data services from mobile operators. This gateway can support LTE/3G/2G depends on respective specifications.

Dynamic IP Address: You may choose this WAN type if you connects a cable modem or a fiber (VDSL modem) for Internet connection. The assigned IP address may be different every time.

Static IP Address: If you get a fixed IP address from your ISP.

PPP over Ethernet: As known as PPPoE. This WAN type is widely used for ADSL connection.

PPTP: This WAN type is more popular in Russia.

L2TP: This WAN type is more popular in Israel.

3.1.1.2.1 3G/4G WAN – 3G/4G

Click on the “**Edit**” button for the 3G/4G WAN interface and you can get the detail WAN settings and then configure the settings as well.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	USB 3G/4G	Failover	3G/4G	Edit

⁹ Different models have different specifications of embedded 3G module. Please refer to specification file for details.

Internet Connection Configuration (WAN - 2)	
Item	Setting
▶ WAN Type	3G/4G ▼

1. **WAN Type:** Choose “3G/4G” from the drop list.

3G/4G WAN Type Configuration	
Item	Setting
▶ Preferred SIM Card	SIM-A First ▼

1. **Preferred SIM Card:** Choose “SIM-A”, “SIM-B”, “SIM-A First” or “SIM-B First” for 3G/4G connection. There are two SIM card slots on this gateway and with four kinds of SIM card usage scenarios, including "SIM-A", "SIM-B", “SIM-A First” and "SIM-B First“. By default, “SIM-A First” scenario is used to connect to mobile system for data transferring. If use “SIM-A First” scenario, the gateway will try to connect to the Internet by using SIM-A card first. And when the connection is broken, gateway system will switch to use SIM-B card for an alternate automatically. System will not switch back to use SIM-A card unless SIM-B connection is also broken. That is, SIM-A and SIM-B are used iteratively, but either one will keep being used for data transferring when current connection is still alive. In the same way, the gateway will try to connect to the Internet by using SIM-B card first if choosing “SIM-B First”. However, when “SIM-A” or “SIM-B” is used, that means the specified SIM slot of card is the ONLY one to be used for negotiation parameters between gateway device and mobile base station.

When you select “SIM-A First” or “SIM-A”, there will be SIM-A Configuration beneath the 3G/4G WAN Type configuration window. However, when you select “SIM-B First” or “SIM-B”, there will be SIM-B Configuration beneath the 3G/4G WAN Type configuration window. All configuration items are the same in SIM-A and SIM-B Configuration. There is also a common configuration for 3G/4G connection.

SIM-A	
▶ Dial-up Profile	☐ Auto-detection ☒ Manual-configuration
▶ Country	Albania ▼
▶ Service Provider	Vodafone ▼
▶ APN	(Optional)
▶ PIN Code	(Optional)
▶ Dial Number	
▶ Account	(Optional)
▶ Password	(Optional)
▶ Authentication	Auto ▼
▶ Primary DNS	(Optional)
▶ Secondary DNS	(Optional)

1. **Dial-up Profile:** After you subscribe 3G/4G data service, your operator will provide some information for you to setup connection, such as APN, dialed number, account or password. If you know this information exactly, you can choose “Manual-configuration” option and type in that information by your own. Otherwise, you can select “Auto-detection” to let this gateway detect automatically. Even you choose “Manual” setting, this gateway will show responding information for your reference after you select country and service provider. If you choose “SIM-A First” or “SIM-B First” for Preferred SIM Card, you need to input dial-up profile for SIM-A and SIM-B respectively.
2. **PIN Code:** Enter PIN code of SIM card if your SIM card needs it to unlock.
3. **Dial Number:** Enter the dialed number that is provided by your ISP.
4. **Account, Password:** Enter Account/Password that is provided by your ISP.
5. **Authentication:** Choose “Auto”, “PAP”, or “CHAP” according to your ISP’s authentication approach. Just keep it with “Auto” if you can’t make sure.
6. **Primary/Secondary DNS:** Enter IP address of Domain Name Server. You can keep them in blank, because most ISP will assign them automatically.

▶ Time Schedule	(0) Always ▼
▶ MTU	0 (0 is Auto)
▶ NAT	☒ Enable
▶ Network Monitoring	☐ Enable ☐ DNS Query ☒ ICMP Checking ☐ Loading Check Check Interval 3 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 10 (Times) Target1 DNS1 Target2 None
▶ IGMP	Disable ▼

1. **Time Schedule:** This option allows you to limit WAN connection available in a certain time period. There is only “**(0) Always**” option available by default. You can add a new time schedule at **System -> Scheduling** menu.
2. **MTU:** MTU refers to Maximum Transmit Unit. Different WAN types of connection will have different value. You can leave it with 0 (Auto) if you are not sure about this setting.
3. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
4. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity. This keep alive feature is also known as Ping Reboot.

Enable: Check the box to do Network Monitoring.

DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicate how often to send keep-alive packet.

Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time period, this gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

5. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.

3.1.1.2.2 Ethernet WAN

Click on the "Edit" button for the Ethernet WAN interface and you can get the detail WAN settings and then configure the settings as well.

Internet Connection List				
Interface Name	Physical Interface	Operation Mode	WAN Type	Action
WAN-1	Ethernet	Always on	Static IP	Edit
WAN-2	3G/4G	Always on	3G/4G	Edit
WAN-3	USB 3G/4G	Failover	3G/4G	Edit

3.1.1.2.2.1 Dynamic IP Address

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	Dynamic IP ▼

Dynamic IP WAN Type Configuration	
Item	Setting
▶ Host Name	(Optional)
▶ ISP Registered MAC Address	Clone
▶ Connection Control	Auto-reconnect (Always on) ▼
▶ MTU	(0 is Auto)
▶ NAT	☒ Enable
▶ Network Monitoring	☒ Enable ☐ DNS Query ☒ ICMP Checking ☐ Loading Check Check Interval 0 (seconds) Check Timeout 0 (seconds) Latency Threshold 0 (ms) Fail Threshold 0 (Times) Target1 DNS1 ▼ Target2 DNS1 ▼
▶ IGMP	Disable ▼
▶ WAN IP Alias	☐ Enable 10.0.0.1

1. **WAN Type:** choose “Dynamic IP” from the drop list.
2. **Host Name:** Optional, required by some ISPs, for example, @Home.
3. **ISP registered MAC Address:** Some ISP would ask you to register a MAC address for Internet connection. In this case, you need to enter the registered MAC address here, or simply press “Clone” button to copy MAC address of your PC to this field.
4. **Connection Control:** Select your connection control scheme from the drop list: “Auto-reconnect (Always-on)”, “Dial-on-demand” or “Manually”. If selecting “Auto-reconnect (Always-on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.
5. **MTU:** Most ISP offers MTU value to users. The default value is 0 (auto).

6. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
7. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

Enable: Check the box to do Network Monitoring.

DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicate how often to send keep-alive packet.

Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time period, this gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

8. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.
9. **WAN IP Alias:** In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

3.1.1.2.2 Static IP Address

Select this option if ISP provides a fixed IP address to you. You will need to enter in the IP address, subnet mask, and gateway address, provided to you by your ISP. Each IP address entered in the fields must be in the appropriate IP form, which is four IP octets separated by a dot (x.x.x.x). The gateway will not accept the IP address if the format is not correct. This does not relate to Fixed IP SIM's.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	Static IP

Static IP WAN Type Configuration	
Item	Setting
▶ WAN IP Address	192.168.121.231
▶ WAN Subnet Mask	255.255.255.0
▶ WAN Gateway	192.168.121.253
▶ Primary DNS	192.168.123.10
▶ Secondary DNS	8.8.8.8
▶ MTU	(0 is Auto)
▶ NAT	☒ Enable
▶ Network Monitoring	☐ Enable ☒ DNS Query ☒ ICMP Checking ☐ Loading Check Check Interval 3 (seconds) Check Timeout 3 (seconds) Latency Threshold 3000 (ms) Fail Threshold 10 (Times) Target1 DNS1 Target2 None
▶ IGMP	Disable
▶ WAN IP Alias	☐ Enable 10.0.0.1

1. **WAN Type:** Choose "Static IP" from the drop list.
2. **WAN IP address/ Subnet Mask/ Gateway:** Enter the IP address, subnet mask, and gateway address which is provided by your ISP.
3. **Primary DNS/ Secondary DNS:** Input the IP address of primary and secondary DNS server that is provided by your ISP. Secondary DNS can be ignored if only one DNS server is provided by your ISP.
4. **MTU:** Most ISP offers MTU value to users. The default value is 0 (auto).
5. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
6. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

Enable: Check the box to do Network Monitoring.

DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicate how often to send keep-alive packet.

Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time period, this gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

7. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.
8. **WAN IP Alias:** In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

3.1.1.2.2.3 PPP over Ethernet

Select this option if your ISP requires you to use a PPPoE connection. This option is typically used for ADSL services.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	PPPoE ▼

PPPoE WAN Type Configuration	
Item	Setting
▶ IPv6 Dual Stack	☐ Enable
▶ PPPoE Account	
▶ PPPoE Password	
▶ Primary DNS	
▶ Secondary DNS	
▶ Connection Control	Auto-reconnect (Always on) ▼
▶ Service Name	(Optional)
▶ Assigned IP Address	(Optional)
▶ MTU	0 (0 is Auto)
▶ NAT	☒ Enable

▶ Network Monitoring	☒ Enable ☐ DNS Query ☒ ICMP Checking ☐ Loading Check Check Interval 0 (seconds) Check Timeout 0 (seconds) Latency Threshold 0 (ms) Fail Threshold 0 (Times) Target1 DNS1 ▼ Target2 DNS1 ▼
▶ IGMP	Disable ▼
▶ WAN IP Alias	☐ Enable 10.0.0.1

1. **WAN Type:** Choose “PPPoE” from the drop list.
2. **IPv6 Dual Stack:** You can enable this option if your ISP provides not only one IPv4 but also one IPv6 address.
3. **PPPoE Account and Password:** The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won’t be displayed on web UI.
4. **Primary DNS/ Secondary DNS:** In most cases, ISP will assign DNS server automatically after PPPoE connection is established. Input the IP address of primary and secondary DNS server manually if required.
5. **Connection Control:** Select your connection control scheme from the drop list: “Auto-reconnect (Always-on)”, “Dial-on-demand” or “Manually”. If selecting “Auto-reconnect (Always-on)”, this gateway will start to establish Internet connection automatically since it’s powered on. It’s recommended to choose this scheme if for mission critical applications to ensure Internet

connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

6. **Service Name/ Assigned IP Address:** ISP may ask you to use a specific service name when connecting PPPoE connection. In some cases, ISP can also provide you a fixed IP address with PPPoE connection. For these cases, you need to add that information in this field.
7. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
9. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

Enable: Check the box to do Network Monitoring.

DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicate how often to send keep-alive packet.

Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn’t receive response within this time period, this gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will

record this keep-alive check is failed if the response time of replied packet is longer than this setting.

Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually..

10. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.
11. **WAN IP Alias:** In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

3.1.1.2.2.4 PPTP

Choose PPTP (Point-to-Point Tunneling Protocol) if your ISP used a PPTP connection. Your ISP will provide you with a username and password.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	PPTP ▼

PPTP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address ▼
▶ Server IP Address / Name	
▶ PPTP Account	
▶ PPTP Password	
▶ Connection ID	(Optional)
▶ Connection Control	Auto-reconnect (Always on) ▼
▶ MTU	0 (0 is Auto)
▶ MPPE	☐ Enable
▶ NAT	☒ Enable
▶ Network Monitoring	☒ Enable ☐ DNS Query ☒ ICMP Checking ☐ Loading Check Check Interval 0 (seconds) Check Timeout 0 (seconds) Latency Threshold 0 (ms) Fail Threshold 0 (Times) Target1 DNS1 ▼ Target2 DNS1 ▼
▶ IGMP	Disable ▼
▶ WAN IP Alias	☐ Enable 10.0.0.1

1. **WAN Type:** Choose “PPTP” from the drop list.
2. **IP Mode:** Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “WAN IP Address”, “WAN Subnet Mask”, and “WAN Gateway” settings provided by your ISP.

▶ IP Mode	Static IP Address ▼
▶ WAN IP Address	
▶ WAN Subnet Mask	
▶ WAN Gateway	

3. **Server IP Address/ Name:** IP address of the PPTP server provided by ISP.
4. **PPTP Account and Password:** The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.
5. **Connection ID:** Optional, input the connection ID if your ISP requires it.
6. **Connection Control:** Select your connection control scheme from the drop list: “Auto-reconnect (Always-on)”, “Dial-on-demand” or “Manually”. If

selecting “Auto-reconnect (Always-on)”, this gateway will start to establish Internet connection automatically since it's powered on. It's recommended to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won't start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won't start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

7. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
8. **MPPE (Microsoft Point-to-Point Encryption):** Enable this option to add encryption on transferred and received data packets. Please check with your ISP to see if this feature is supported or not.
9. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
10. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

Enable: Check the box to do Network Monitoring.

DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicate how often to send keep-alive packet.

Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn't receive response within this time

period, this gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will record this keep-alive check is failed if the response time of replied packet is longer than this setting.

Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

11. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.
12. **WAN IP Alias:** In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

3.1.1.2.2.5 L2TP

Choose L2TP (Layer 2 Tunneling Protocol) if your ISP used a L2TP connection. Your ISP will provide you with a username and password.

Internet Connection Configuration (WAN - 1)	
Item	Setting
▶ WAN Type	L2TP ▼

L2TP WAN Type Configuration	
Item	Setting
▶ IP Mode	Dynamic IP Address ▼
▶ Server IP Address / Name	
▶ L2TP Account	
▶ L2TP Password	
▶ Connection Control	Auto-reconnect (Always on) ▼
▶ MTU	0 (0 is Auto)
▶ MPPE	☐ Enable
▶ NAT	☒ Enable
▶ Network Monitoring	☒ Enable ☐ DNS Query ☒ ICMP Checking ☐ Loading Check Check Interval 0 (seconds) Check Timeout 0 (seconds) Latency Threshold 0 (ms) Fail Threshold 0 (Times) Target1 DNS1 Target2 DNS1
▶ IGMP	Disable ▼
▶ WAN IP Alias	☐ Enable 10.0.0.1

1. **WAN Type:** Choose “L2TP” from the drop list.
2. **IP Mode:** Please check the IP mode your ISP assigned, and select “Static IP Address” or “Dynamic IP Address” accordingly. If you select “Static IP Address” option, you have to specify additional “IP Address”, “Subnet Mask”, and “WAN Gateway IP” settings provided by your ISP.

▶ IP Mode	Static IP Address ▼
▶ WAN IP Address	
▶ WAN Subnet Mask	
▶ WAN Gateway	

3. **Server IP Address / Name:** IP address of the L2TP server provided by ISP.
4. **L2TP Account and Password:** The account and password your ISP assigned to you. Please note the account and password is case sensitive. For security concern, the password you input won't be displayed on web UI.
5. **Connection Control:** Select your connection control scheme from the drop list: “Auto-reconnect (Always-on)”, “Dial-on-demand” or “Manually”. If selecting “Auto-reconnect (Always-on)”, this gateway will start to establish Internet connection automatically since it's powered on. It's recommended

to choose this scheme if for mission critical applications to ensure Internet connection is available all the time. If choosing “Dial-on-demand”, this gateway won’t start to establish Internet connection until local data is going to be sent to WAN side. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time. If choosing “Manually”, this gateway won’t start to establish WAN connection until you press “Connect” button on web UI. After that, this gateway will disconnect WAN connection if idle time reaches value of Maximum Idle Time.

6. **MTU:** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
7. **MPPE (Microsoft Point-to-Point Encryption):** Enable this option to add encryption on transferred and received data packets. Please check with your ISP to see if this feature is supported or not.
8. **NAT:** By default, it is enabled. If you disable this option, there will be no NAT mechanism between LAN side and WAN side.
9. **Network Monitoring:** You can do preferred settings by using this feature to monitor the connection status of WAN interface. Checking mechanism depends on several parameters defined here. The network monitoring provides the WAN interface status and then system can prevent embedded 3G/LTE modem from some sort of auto-timeout and disconnects from the Internet after a period of inactivity.

Enable: Check the box to do Network Monitoring.

DNS Query/ICMP Checking: Do the keep alive through DNS query packets or ICMP packets.

Loading Checking: The response time of replied keep-alive packets may increase when WAN bandwidth is fully occupied. To avoid keep-alive feature work abnormally, enable this option will stop sending keep-alive packets when there are continuous incoming and outgoing data packets passing through WAN connection.

Check Interval: Indicate how often to send keep-alive packet.

Check Timeout: Set allowance of time period to receive response of keep-alive packet. If this gateway doesn’t receive response within this time period, this gateway will record this keep alive is failed.

Latency Threshold: Set acceptance of response time. This gateway will

record this keep-alive check is failed if the response time of replied packet is longer than this setting.

Fail Threshold: Times of failed checking. This WAN connection will be recognized as broken if the times of continuous failed keep-alive checking equals to this value.

Target1/Target2: Set host that is used for keep alive checking. It can be DNS1, DNS2, default Gateway, or other host that you need to input IP address manually.

10. **IGMP:** Enable or disable multicast traffics from Internet. You may enable as auto mode or select by IGMP v1, IGMP v2, IGMP v3 or Auto.
11. **WAN IP Alias:** In some cases, ISP will provide you another fixed IP address for management purpose. You can enter that IP address in this field.

3.1.1.3 Load Balance

This device support multi-WAN load balance function and more than one WAN interface can access to Internet at a time. The load balance function can help you to manage the outbound traffics and to maximize the utilization of available bandwidth.

Physical Interface Internet Setup Load Balance	
Configuration	
Item	Setting
▶ Load Balance	☒ Enable
▶ Load Balance Strategy	By Smart Weight ▼

1. **Load Balance:** Enable or disable the load balance function.
2. **Load Balance Strategy:** Once you enabled the load balance function, you have to further configure which strategy is to be applied for load balancing the outbound traffics. There are three load balance strategy: “**By Smart Weight**”, “**By Priority**”, and “**By User Policy**”.

By Smart Weight

Configuration	
Item	Setting
▶ Load Balance	☒ Enable
▶ Load Balance Strategy	By Smart Weight ▼

If you choose the “**By Smart Weight**” strategy, No any other setting is required. This

device will automatically allocate the outbound traffics to each WAN interface.

By Priority

Configuration	
Item	Setting
▶ Load Balance	☒ Enable
▶ Load Balance Strategy	By Priority ▼

Priority	
WAN	Priority
▶ WAN - 1	0 %
▶ WAN - 2	0 %

If you choose the “**By Priority**” strategy, you have to further specify the outbound traffic percentage for each WAN interface. The load balancing mechanism will follow these settings to allocate proper traffics for each WAN to access the internet.

By User Policy

Configuration	
Item	Setting
▶ Load Balance	☒ Enable
▶ Load Balance Strategy	By User Policy ▼

If you choose the “**By User Policy**” strategy, you have to create the expected policies one by one. Click the “**add**” button to add your load balance policy.

User Policy List						
ID	Source IP Address	Destination IP Address	Destination Port	WAN Interface	Enable	Actions
Add Delete						

You can manage the outbound traffics flow and the force specific traffics to access Internet through designated WAN interface. For those traffics not covered in the user policy rules, the device will allocate the WAN interface by applying “Smart Weight” mechanism simultaneously.

User Policy Configuration	
Item	Setting
▶ Source IP Address	Any ▼
▶ Destination IP Address	Any ▼
▶ Destination Port	All ▼
▶ Protocol	Both ▼
▶ WAN Interface	WAN - 1 ▼
▶ Policy	☒ Enable

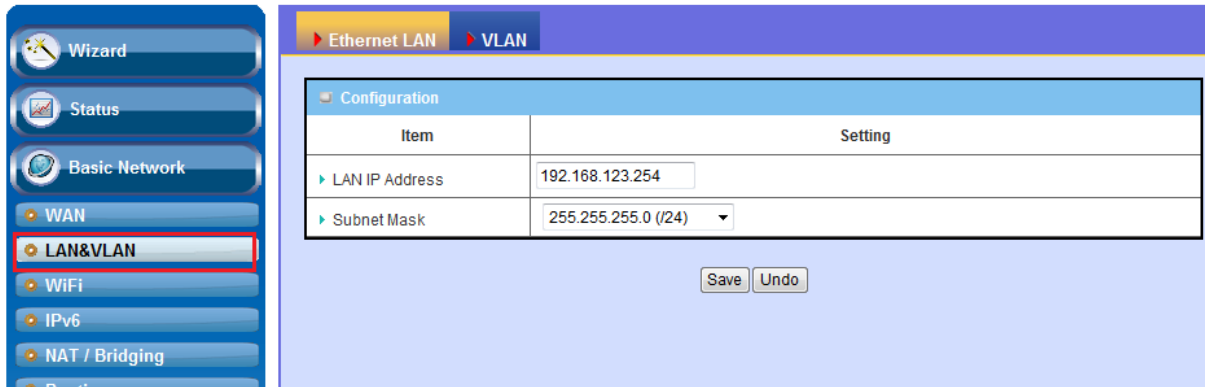
- 1. Source IP Address:** Enter the expected Source IP Address for the load balance policy. It can be "Any", "Subnet", "IP Range", or "Single IP". Just choose one type of the source IP address, and specify its value as well. If you don't want to specify a certain source IP address for this policy, just leave it as "Any".
- 2. Destination IP Address:** Enter the expected Destination IP Address for the load balance policy. It can be "Any", "Subnet", "IP Range", "Single IP", or "Domain Name". Just choose one type of the destination IP address, and specify its value as well. If you don't want to specify a certain destination IP address for this policy, just leave it as "Any".
- 3. Destination Port:** Enter the expected Destination Port number for the load balance policy. It can be "All", "Port Range", "Single Port", or "Well-known Applications". Just choose one type of the destination port, and specify its value as well. If you don't want to specify a certain destination port for this policy, just leave it as "All".
- 4. Protocol:** Enter the expected protocol type for the load balance policy. It can be "TCP", "UDP" or "Both". If you don't want to specify a certain protocol type for this policy, just leave it as "Both".
- 5. WAN Interface:** Identify which WAN interface is to be selected for accessing the Internet if all of above source and destination criteria are matched for the outbound traffics.
- 6. Policy:** Enable or disable this user policy.

3.1.2 LAN & VLAN Setup

This device is equipped with four Fast Ethernet LAN¹⁰ ports as to connect your local devices via Ethernet cables. Besides, VLAN function is provided to organize your

¹⁰ The 1st Ethernet port will be configured to WAN port if you have set Ethernet WAN.

local networks.

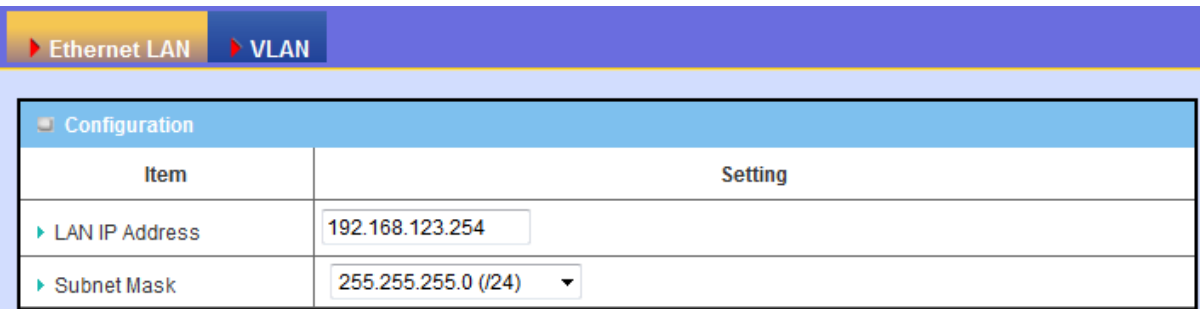


Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

Save Undo

3.1.2.1 Ethernet LAN

Please follow the following instructions to do IPv4 Ethernet LAN Setup.



Item	Setting
LAN IP Address	192.168.123.254
Subnet Mask	255.255.255.0 (/24)

- 1. LAN IP Address:** The local IP address of this device. The computer on your network must use the LAN IP address of this device as their Default Gateway. You can change it if necessary. It's also the IP address of web UI. If you change it, you need to type new IP address in the browser to see web UI.
- 2. Subnet Mask:** Input your Subnet mask. Subnet mask defines how many clients are allowed in one network or subnet. The default subnet mask is 255.255.255.0 (/24), and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

255.0.0.0 (/8)
255.128.0.0 (/9)
255.192.0.0 (/10)
255.224.0.0 (/11)
255.240.0.0 (/12)
255.248.0.0 (/13)
255.252.0.0 (/14)
255.254.0.0 (/15)
255.255.0.0 (/16)
255.255.128.0 (/17)
255.255.192.0 (/18)
255.255.224.0 (/19)
255.255.240.0 (/20)
255.255.248.0 (/21)
255.255.252.0 (/22)
255.255.254.0 (/23)
255.255.255.0 (/24)
255.255.255.128 (/25)
255.255.255.192 (/26)
255.255.255.224 (/27)
255.255.255.240 (/28)
255.255.255.248 (/29)
255.255.255.252 (/30)

3.1.2.2 VLAN

This section provides a brief description of VLANs and explains how to create and modify virtual LANs which are more commonly known as VLANs. A VLAN is a logical network under a certain switch or router device to group lots of client hosts with a specific VLAN ID. This device supports both Port-based VLAN and Tag-based VLAN. In Port-based VLAN, all client hosts belong to the same group by transferring data via some physical ports that are tagged with same VLAN ID in the device. The ports of a VLAN form an independent traffic domain in which the traffic generated by the nodes remains within the VLAN. However, in Tag-based VLAN, all packets with same VLAN ID will be treated as the same group of them and own same access property and QoS property. It is especially useful when individuals of a VLAN group are located at different location.

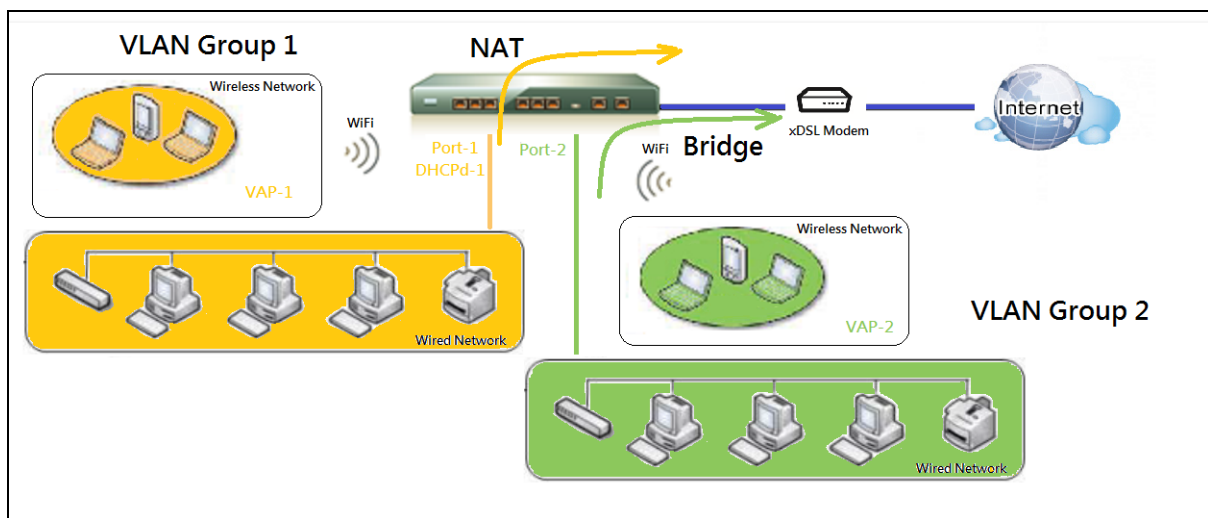
The VLAN function allows you to divide local network into different “virtual LANs”. In some cases, ISP may need router to support “VLAN tag” for certain kinds of services (e.g. IPTV) to work properly. In some cases, SMB departments are separated and located at any floor of building. All client hosts in same department should own common access property and QoS property. You can select either one operation mode, port-based VLAN or tag-based VLAN, and then configure according to your network configuration.

3.1.2.2.1 VLAN Scenarios

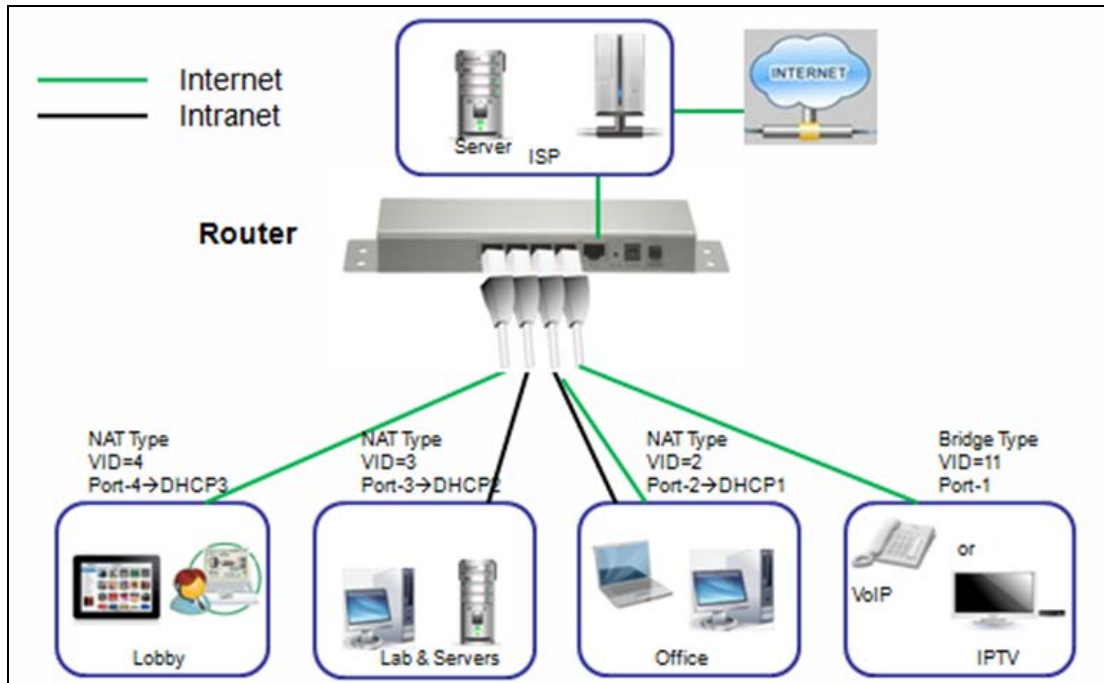
There are some common VLAN scenarios as follows:

- Port-Based VLAN Tagging for Differentiated Services

Port-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together for differentiated services like Internet surfing, multimedia enjoyment, VoIP talking, and so on. Two operation modes, NAT and Bridge, can be applied to each VLAN group. One DHCP server is allocated for an NAT VLAN group to let group host member get its IP address. Thus, each host can surf Internet via the NAT mechanism of business access gateway. At bridge mode, Intranet packet flow was delivered out WAN trunk port with VLAN tag to upper link for different services.

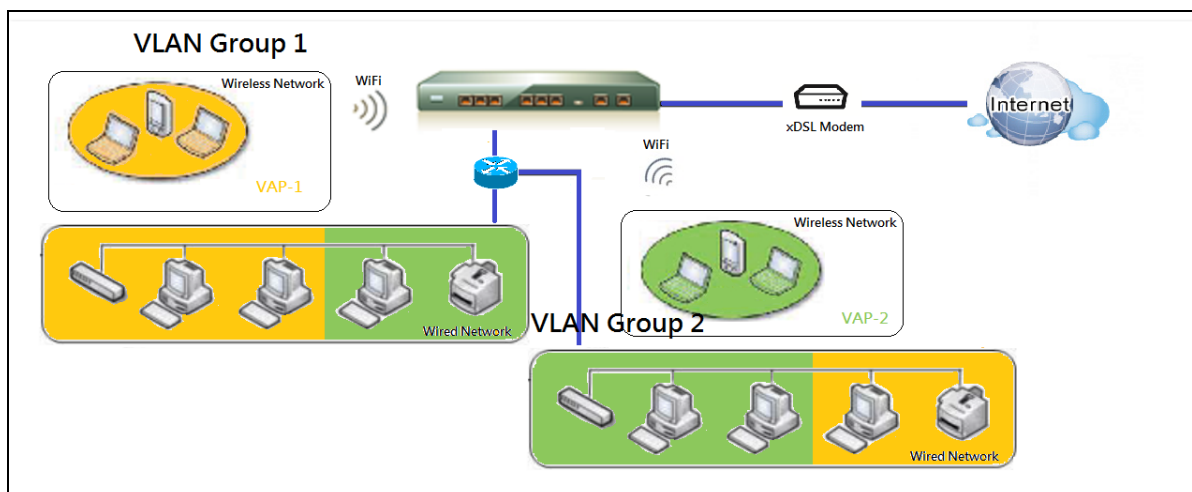


A port-based VLAN is a group of ports on an Ethernet or Virtual APs of Wired or Wireless Gateway that form a logical Ethernet segment. Following is an example. In SMB or a company, administrator schemes out 4 segments, Lobby, Lab & Servers, Office and VoIP & IPTV. In a Wireless Gateway, administrator can configure Lobby segment with VLAN ID 4. The VLAN group includes Port-4 and VAP-8 (SSID: Guest) with NAT mode and DHCP-3 server equipped. He also configure Lab & Servers segment with VLAN ID 3. The VLAN group includes Port-3 with NAT mode and DHCP-2 server equipped. However, he configure Office segment with VLAN ID 2. The VLAN group includes Port-2 and VAP-1 (SSID: Staff) with NAT mode and DHCP-1 server equipped. At last, administrator also configure VoIP & IPTV segment with VLAN ID 11. The VLAN group includes Port-1 with bridge mode to WAN interface as shown at following diagram.



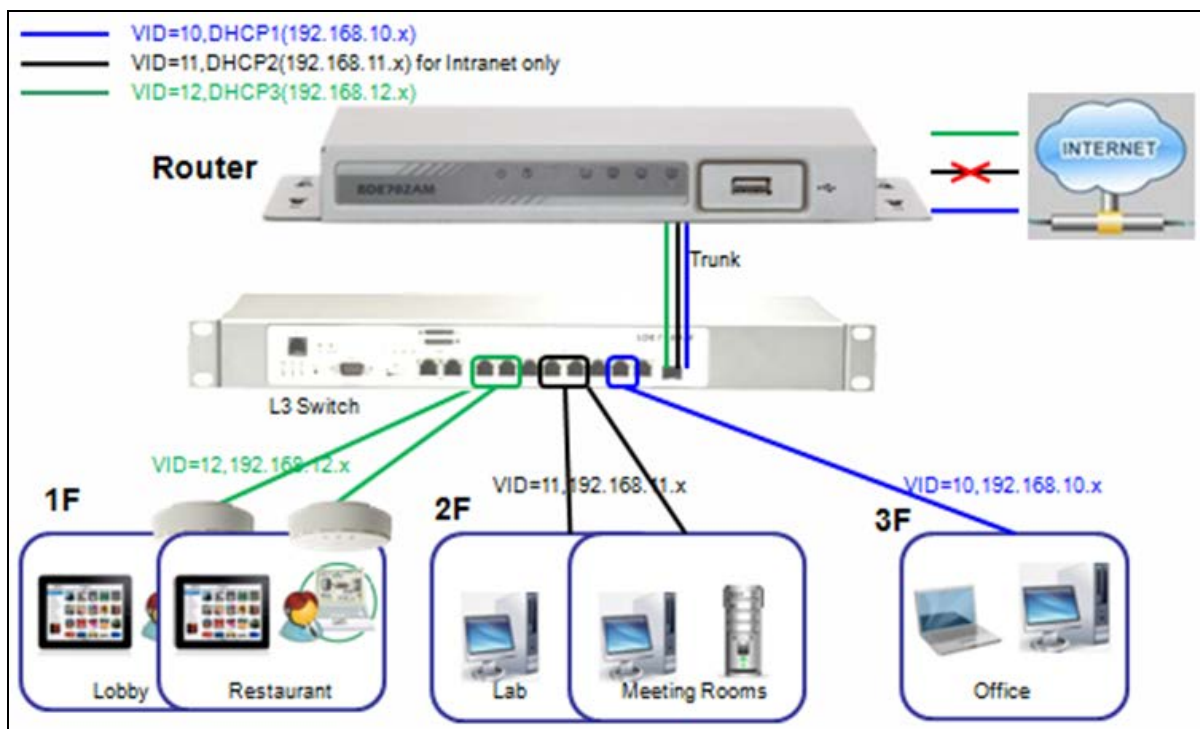
- Tag-based VLAN Tagging for Location-free Departments

Tag-based VLAN function can group Ethernet ports, Port-1 ~ Port-4, and WiFi Virtual Access Points, VAP-1 ~ VAP-8, together with different VLAN tags for deploying department subnets in Intranet. All packet flows can carry with different VLAN tags even at the same physical port for Intranet. These flows can be directed to different destination because they have differentiated tags. The approach is very useful to group some hosts in different geographic location to be a same department.



Tag-based VLAN is also called a VLAN Trunk. The VLAN Trunk collects all packet flows with different VLAN IDs from Router device and delivers them in the Intranet. VLAN membership in a tagged VLAN is determined by VLAN ID information within

the packet frames that are received on a port. Administrator can further use a VLAN switch to separate the VLAN trunk to different groups based on VLAN ID. Following is an example. In SMB or a company, administrator schemes out 3 segments, Lobby & Restaurant, Lab & Meeting Rooms and Office. In a Security VPN Gateway, administrator can configure Lobby & Restaurant segment with VLAN ID 12. The VLAN group is equipped with DHCP-3 server to construct a 192.168.12.x subnet. He also configure Lab & Meeting Rooms segment with VLAN ID 11. The VLAN group is equipped with DHCP-2 server to construct a 192.168.11.x subnet for Intranet only. That is, any client host in VLAN 11 group can't access the Internet. However, he configure Office segment with VLAN ID 10. The VLAN group is equipped with DHCP-1 server to construct a 192.168.10.x subnet. In this example, VLAN 10 and 12 groups can access the Internet as following diagram.



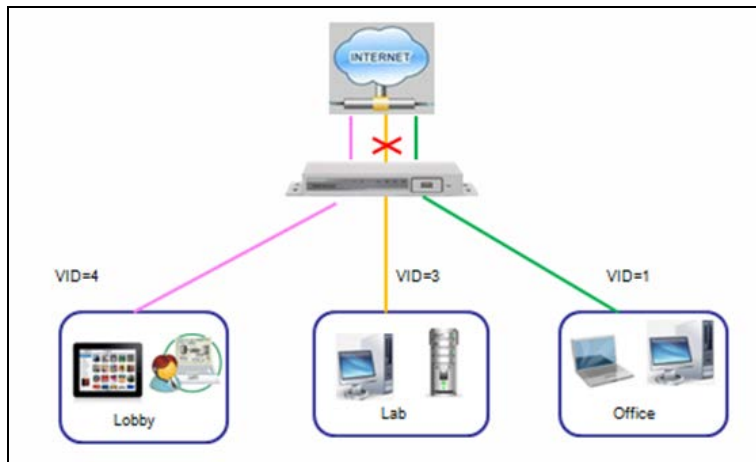
- VLAN Group Access Control

Administrator can specify the Internet access right for all VLAN groups. He also can configure which VLAN groups can communicate each other.

VLAN Group Internet Access

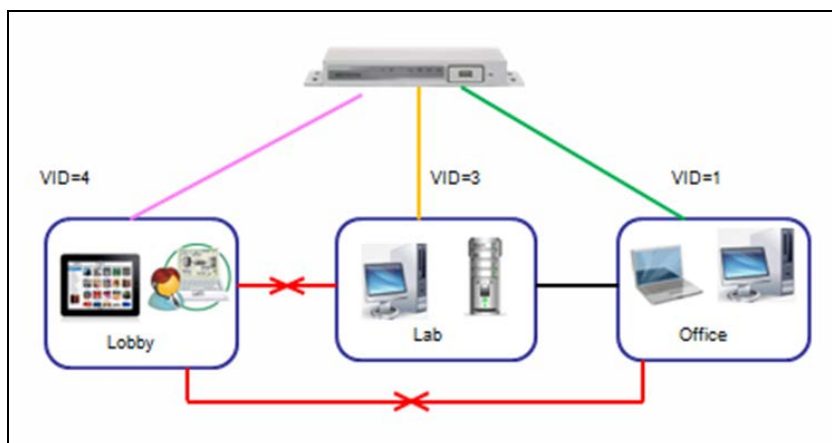
Administrator can specify members of one VLAN group to be able to access Internet or not. Following is an example that VLAN groups of VID is 1 and 4 can access Internet but the one with VID is 3 can't. That is, visitors in Lobby and staffs in office can access Internet. But ones in Lab can't since security issue. Servers in Lab serve

only for trusted staffs or are accessed in secure tunnels.



Inter VLAN Group Routing:

In Port-based tagging, administrator can specify member hosts of one VLAN group to be able to communicate with the ones of another VLAN group or not. This is a communication pair, and one VLAN group can join many communication pairs. But communication pair has not the transitive property. That is, A can communicate with B, and B can communicate with C, that doesn't mean A can communicate with C. An example is shown at following diagram. VLAN groups of VID is 1 and 3 can access each other but the ones between VID 3 and VID 4 and between VID 1 and VID 4 can't.



3.1.2.2.2 Port-Based VLAN

A port-based VLAN is a group of ports on an Ethernet switch or router that form a logical Ethernet segment. There are four LAN ports and up to eight virtual APs in this device, so you can have various VLAN configurations to organization the available LAN ports and virtual APs if required.

Configuration [Help]

Item

Setting

VLAN Type

Port-based

Port-based VLAN List

Port	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action
Port1	NAT	1	X	DHCP1/Enable 192.168.75.0/0	X	0	Edit
Port2	NAT	1	X	DHCP1/Enable 192.168.75.0/0	X	0	Edit
Port3	NAT	2	X	DHCP2/Disable 192.168.2.0/0	X	0	Edit
Port4	NAT	2	X	DHCP2/Disable 192.168.2.0/0	X	0	Edit
Virtual AP	NAT/Bridge	VLAN ID	Tx TAG	DHCP Server	Available WAN	WAN VID	Action
VAP1	NAT	1	X	DHCP1/Enable 192.168.75.0/0	X	0	Edit
VAP2	NAT	1	X	DHCP1/Enable 192.168.75.0/0	X	0	Edit
VAP3	NAT	1	X	DHCP1/Enable 192.168.75.0/0	X	0	Edit
VAP4	NAT	1	X	DHCP1/Enable 192.168.75.0/0	X	0	Edit
VAP5	NAT	2	X	DHCP2/Disable 192.168.2.0/0	X	0	Edit
VAP6	NAT	2	X	DHCP2/Disable 192.168.2.0/0	X	0	Edit
VAP7	NAT	2	X	DHCP2/Disable 192.168.2.0/0	X	0	Edit
VAP8	NAT	2	X	DHCP2/Disable 192.168.2.0/0	X	0	Edit

Port-based VLAN Summary

VLAN IDs	Members	NAT/Bridge	DHCP Server	Bridged WAN	Tx Tag
1	Port1, Port2, VAP-1, VAP-2, VAP-3, VAP-4	NAT	DHCP1	X	No
2	Port3, Port4, VAP-5, VAP-6, VAP-7, VAP-8	NAT	DHCP2	X	No

[Save](#)
[VLAN Routing Group](#)
[Reboot](#)

By default, all the 4 LAN ports and 8 virtual APs belong to one VLAN, and this VLAN is a NAT type network, all the local device IP addresses are allocated by DHCP server 1. If you want to divide them into different VLANs, click on the “Edit” button related to each port.

- Type:** Select “NAT” or “Bridge” to identify if the packets are directly bridged to the WAN port or processed by NAT mechanism.
- LAN VID:** Specify a VLAN identifier for this port. The ports with the same VID are in the same VLAN group.
- Tx TAG:** If ISP requests a “VLAN Tag” with your outgoing data, please check the checkbox of “Tx TAG”.
- DHCP Server:** Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.
- WAN VID:** The VLAN Tag ID that come from the ISP service. For NAT type VLAN, no WAN VLAN tag is allowed and the value is forced to “0”; For Bridge type VLAN, You have to specify the VLAN Tag value that is provided by your ISP.
- VLAN Routing Group:**

Summary			
LAN VALN Settings			
Ethernet	NAT/Bridge	VLAN ID	Tx TAG
Port1	NAT	1	☐
Port2	NAT	1	☐
Port3	NAT	2	☐
Port4	Bridge	11	☒
Wireless LAN VLAN Settings			
Virtual AP	NAT/Bridge	VLAN ID	Tx TAG
VAP1	NAT	1	☐
VAP2	NAT	1	☐
VAP3	NAT	1	☐
VAP4	NAT	1	☐
VAP5	NAT	2	☐
VAP6	NAT	2	☐
VAP7	NAT	2	☐
VAP8	NAT	2	☐
VLAN Group Internet Access Definition			
VLAN IDs	Members	Internet Access(WAN)	
1	Port1, Port2, VAP1, VAP2, VAP3, VAP4	Allow Edit	
2	Port3, VAP5, VAP6, VAP7, VAP8	Deny	
Inter VLAN Group Routing			
VLAN IDs	Members	Action	
1, 2	Port1, Port2, Port3	Edit	
		Edit	
		Edit	
		Edit	
Save Back Reboot			
Saved! The change doesn't take effect until router is rebooted.			

Above configuration example supports 3 access policies. The first one is Internet Access Policy that includes Port-1, Port-2, VAP-1 ~ VAP-4. All client hosts via these interfaces can access the Internet. The second policy is Intranet access Policy that includes Port-3 and VAP-5~ VAP-8. All client hosts via these interfaces can't access the Internet. But the Ethernet client hosts of VLAN 1 and 2 groups can communicate each other. About the configuration of inter-VAP routing, please refer to Basic Network >> WiFi section. The last one policy is the Bridge to WAN Policy that includes only Port-4.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.1.2.2.3 Tag-Based VLAN

The second type of VLAN is the tag-based VLAN. VLAN membership in a tagged VLAN is determined by VLAN information within the packet frames that are received on a port. This differs from a port-based VLAN, where the port VIDs assigned to the ports determine VLAN membership.

When the device receives a frame with a VLAN tag, referred to as a tagged frame, the device forwards the frame only to those ports that share the same VID.

Tag-based ▼

Tag-based VLAN List
Add
Delete

VLAN ID	Internet	Port	VAP	DHCP Server	Actions
1	☒	☒ 1 ☒ 2 ☒ 3 ☒ 4	☒ 1 ☒ 2 ☒ 3 ☒ 4 ☒ 5 ☒ 6 ☒ 7 ☒ 8	DHCP-1	Edit

Tag-based VLAN Summary

Port	VLAN IDs
Port1	1
Port2	1
Port3	1
Port4	1

By default, all the LAN ports and virtual APs belong to one VLAN, and this VLAN ID is forced to “1”. It is a special tag based VLAN for device to operated, there is no tag required for this default VLAN ID.

If you want to configure your own tag-based VLANs, click on the “Edit” checkbox on a new VLAN ID row.

1. **VLAN ID:** Specify a VLAN tag for this VLAN group. The ports with the same VID are in the same VLAN group.
2. **Internet:** Specify whether this VLAN group can access Internet or not. If it is checked, all the packet will be un-tagged before it is forward to Internet, and all the packets from Internet will be tagged with the VLAN ID before it is forward to the destination belongs to this configuring VLAN group in the Intranet.
3. **Port-1 ~ Port-4, VAP-1 ~ VAP-8:** Specify whether they belong to the VLAN group or not. You just have to check the boxes for dedicated ports.
4. **DHCP Server:** Specify a DHCP server for the configuring VLAN. This device provides up to 4 DHCP servers to serve the DHCP requests from different VLANs.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3 WiFi Setup

The gateway supports 2.4GHz 802.11n 2Tx2R MIMO WiFi, and also can be back compatible to 802.11b/g clients. WiFi settings allow you to set the wireless LAN configuration items. When the wireless configuration is done, your WiFi LAN is ready to support your local WiFi devices such as your laptop PC, smart phone, tablet, wireless printer and some portable wireless devices.

Configuration > Advanced Configuration

Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band
WPS	2.4G WPS Setup

2.4G WiFi Configuration

Item	Setting
WiFi Module	☒ Enable
WiFi Operation Mode	AP Router Mode
Green AP	☐ Enable
Multiple AP Names & Enable & Max. STA	VAP 1 ☒ Enable Max. Sta ☐ Enable (1~16)
Time Schedule	(0) Always
Network ID (SSID) & Broadcast	JP.75 Broadcast ☒ Enable
WLAN Partition	☐ Enable
Channel	Auto
WiFi System	802.11b/g/n Mixed
Authentication	Auto 802.1x ☐ Enable
Encryption	None

Save Undo

3.1.3.1 WiFi Configuration

This device is equipped with IEEE802.11b/g/n 2Tx2R wireless radio, you have to configure 2.4G Hz operation band's wireless settings and then activate your WLAN.

Configuration > Wireless Client List > Advanced Configuration

Basic Configuration [Help]

Item	Setting
Operation Band	2.4G Single Band
WPS	2.4G WPS Setup

2.4G WiFi Configuration

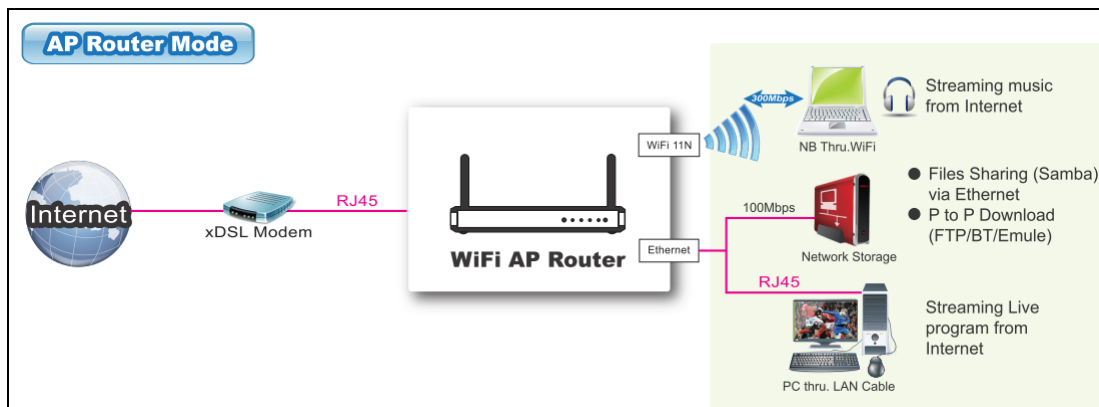
Item	Setting
WiFi Module	☒ Enable
WiFi Operation Mode	AP Router Mode
Green AP	☐ Enable
Multiple AP Names & Enable & Max. STA	VAP 1 ☒ Enable Max. Sta ☐ Enable (1~16)
Time Schedule	(0) Always
Network ID (SSID) & Broadcast	JP.75 Broadcast ☒ Enable
WLAN Partition	☐ Enable
Channel	Auto
WiFi System	802.11b/g/n Mixed
Authentication	Auto 802.1x ☐ Enable
Encryption	None

Save Undo

There are several wireless operation modes provided by this device. They are: “**AP Router Mode**”, “**WDS Hybrid Mode**”, and “**WDS Only Mode**”. You can choose the expected mode from the wireless operation mode list.

3.1.3.1.1 AP Router Mode

This mode allows you to get your wired and wireless devices connected with NAT.



In this mode, this gateway is working as a WiFi AP, but also a WiFi hotspot. It means local WiFi clients can associate to it, and go to Internet. With its NAT mechanism, all of wireless clients don't need to get public IP addresses from ISP.

Basic Configuration [Help]	
Item	Setting
▶ Operation Band	2.4G Single Band ▼
▶ WPS	2.4G WPS Setup

- 1. Operation Band:** Select the WiFi operation band that you want to configure. But the device supports only 2.4G single WiFi band.
- 2. WPS:** Click on the button to setup WPS.

2.4G WiFi Configuration	
Item	Setting
▶ WiFi Module	☒ Enable
▶ WiFi Operation Mode	AP Router Mode ▼
▶ Green AP	☐ Enable
▶ Multiple AP Names & Enable & Max. STA	VAP 1 ▼ ☒ Enable Max.Sta ☐ Enable (1~16)
▶ Time Schedule	(0) Always ▼
▶ Network ID (SSID) & Broadcast	JP.75 Broadcast ☒ Enable
▶ WLAN Partition	☐ Enable
▶ Channel	Auto ▼
▶ WiFi System	802.11b/g/n Mixed ▼
▶ Authentication	Auto ▼ 802.1x ☐ Enable
▶ Encryption	None ▼

- 1. Wireless Module:** Enable the wireless function.
- 2. Wireless Operation Mode:** Choose “AP Router Mode” from the drop list.
- 3. Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffic. By default, it is disabled.

4. **Multiple AP Names:** This device supports up to 8 SSIDs for you to manage your wireless network. You can select VAP-1 ~ VAP-8 and configure each wireless network if it is required.
5. **Time Schedule:** The wireless radio can be turn on according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled. If you want to add a new schedule rule, please go to **System** -> **Scheduling** menu.
6. **Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is "default")
7. **SSID Broadcast:** The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as "Disable", the wireless clients can't find the device from beacons.
8. **WLAN Partition:** You can check the WLAN Partition function to separate the wireless clients. The wireless clients can't communicate each other, but they can access the internet and other Ethernet LAN devices.
9. **Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection. It's recommended to choose a channel that is not used in your environment to reduce radio interference.
10. **Wireless System:** This gateway supports 802.11a/b/g/n modes. For 2.4GHz operation band, you can also choose "N only", "G/N mixed" or "B/G/N mixed", and for 5GHz operation band, you can choose "A only", "N only", or "A/N mixed" according to your requirement. The factory default setting is "B/G/N mixed" for 2.4GHz and "A/N mixed" for 5GHz. But the device supports only 2.4GHz.
11. **Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK, WPA, WPA2-PSK, WPA2, WPA-PSK/WPA2-PSK, or WPA/WPA2.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration. In this mode you can enable 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port and shared key of RADIUS server here.

▶ Authentication	Open ▼	802.1x ☒ Enable
▶ RADIUS Server	RADIUS Server IP	0.0.0.0
	RADIUS Server Port	1812
	RADIUS Shared Key	

In this mode, you can only choose “None” or “WEP” in the encryption field.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The gateway will select appropriate authentication method according to WiFi client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don't need additional RADIUS server for user authentication.

- **WPA**

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

- **WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don't need additional RADIUS server for user authentication.

- **WPA2**

Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII

characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”.

- **WPA-PSK/WPA2-PSK**

If some of wireless clients can only support WPA-PSK, but most of them can support WPA2-PSK. You can choose this option to support both of them. Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. In this mode, you don't need additional RADIUS server for user authentication.

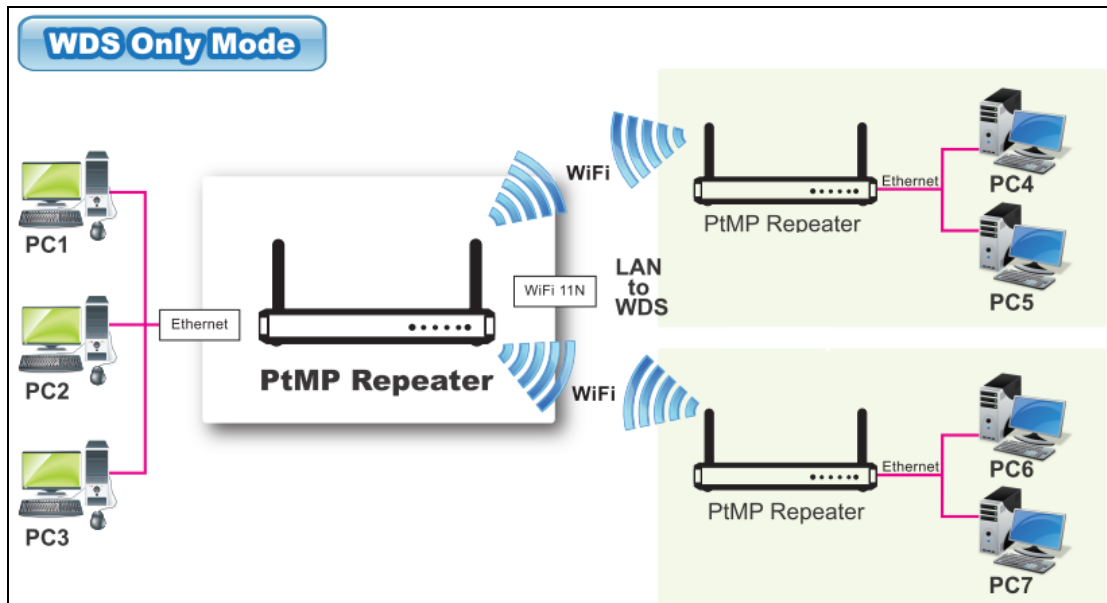
- **WPA/WPA2**

If some of wireless clients can only support WPA, but most of them can support WPA2. You can choose this option to support both of them. Select Encryption mode and enter RADIUS Server related information. You have to specify the IP address and port number for the RADIUS Server, and then fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the shared key. The key value is shared by the RADIUS server and this router. This key value must be consistent with the key value in the RADIUS server.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.2 WDS Only Mode

While acting as a wireless bridge, Wireless Repeater 1 and Wireless Repeater 2 can communicate with each other through wireless interface (with WDS). Thus all stations can communicate each other.



2.4G WiFi Configuration	
Item	Setting
WiFi Module	☒ Enable
WiFi Operation Mode	WDS Only Mode
Lazy Mode	☒ Enable
Green AP	☐ Enable
Channel	Auto
Authentication	Auto
Encryption	None

- Wireless Module:** Enable the wireless function.
- Wireless Operation Mode:** Choose “WDS Only Mode” from the drop list.
- Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.
- Green AP:** Enable the Green AP function to reduce the power consumption when there are no wireless traffics.
- Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. The factory default setting is auto channel selection.
- Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK and WPA2-PSK.
 - **Open**
Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the

AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration. In this mode you can enable 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port and shared key of RADIUS server here.

▶ Authentication	Open ▼	802.1x ☒ Enable
▶ RADIUS Server	RADIUS Server IP	0.0.0.0
	RADIUS Server Port	1812
	RADIUS Shared Key	

In this mode, you can only choose “None” or “WEP” in the encryption field.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The gateway will select appropriate authentication method according to WiFi client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don't need additional RADIUS server for user authentication.

- **WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don't need additional RADIUS server for user authentication.

- 7. Scan Remote AP's MAC List:** If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one. Click on the “Scan” button to get the available AP's MAC list automatically and select the expected item and copy its MAC address to the Remote AP MAC 1~4 one by one.

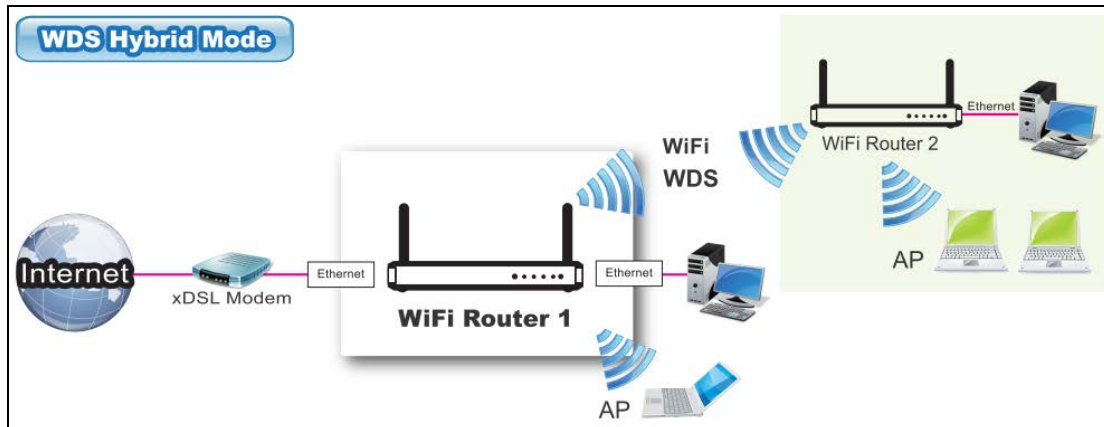
▶ Scan Remote AP's MAC List	Scan					
Remote AP MAC1	☒ Copy MAC to Here					
Remote AP MAC2	☐ Copy MAC to Here					
Remote AP MAC3	☐ Copy MAC to Here					
Remote AP MAC4	☐ Copy MAC to Here					
Save Undo						
Wireless AP List						
SSID	Channel	Quality	Authentication	Encryption	MAC Address	Select

8. Remote AP MAC 1 ~ Remote AP MAC 4: If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.3 WDS Hybrid Mode

WDS (Wireless Distributed System) Hybrid function let this access point acts as a wireless LAN access point and a repeater at the same time. Users can use this feature to build up a large wireless network in a large space like airports, hotels and schools ...etc.



2.4G WiFi Configuration	
Item	Setting
▶ WiFi Module	☒ Enable
▶ WiFi Operation Mode	WDS Hybrid Mode ▼
▶ Lazy Mode	☒ Enable
▶ Green AP	☐ Enable
▶ Multiple AP Names & Enable & Max. STA	VAP 1 ▼ ☒ Enable Max.Sta ☒ Enable 12 (1~16)
▶ Time Schedule	(0) Always ▼
▶ Network ID (SSID) & Broadcast	JP.75 Broadcast ☒ Enable
▶ WLAN Partition	☐ Enable
▶ Channel	Auto ▼
▶ Authentication	Auto ▼
▶ Encryption	None ▼

- 1. Wireless Module:** Enable the wireless function.
- 2. Wireless Operation Mode:** Choose “WDS Hybrid Mode” from the drop list.
- 3. Lazy Mode:** This device support the Lazy Mode to automatically learn the MAC address of WDS peers, you don't have to input other peer AP's MAC address. However, not all the APs can be set to enable the Lazy Mode simultaneously; at least there must be one AP with all the WDS peers' MAC address filled.
- 4. Green AP:** Enable the Green AP function to reduce the power consumption when there is no wireless traffics.
- 5. Multiple AP Names:** This device supports up to 8 SSIDs for you to manage your wireless network. You can select VAP-1 ~ VAP-8 and configure each wireless network if it is required.
- 6. Time Schedule:** The wireless radio can be turn on according to the schedule rule you specified. By default, the wireless radio is always turned on when the wireless module is enabled. If you want to add a new schedule rule, please go to **System** -> **Scheduling** menu.
- 7. Network ID (SSID):** Network ID is used for identifying the Wireless LAN (WLAN). Client stations can roam freely over this device and other Access Points that have the same Network ID. (The factory default setting is “default”)
- 8. SSID Broadcast:** The router will broadcast beacons that have some information, including SSID so that wireless clients can know how many AP devices by scanning the network. Therefore, if this setting is configured as “Disable”, the wireless clients can't find the device from beacons.
- 9. Channel:** The radio channel number. The permissible channels depend on the Regulatory Domain. This channel number needs to be same as the channel number of peer AP.
- 10. Authentication & Encryption:** You may select one of the following authentications to secure your wireless network: Open, Shared, Auto, WPA-PSK

and WPA2-PSK.

- **Open**

Open system authentication simply consists of two communications. The first is an authentication request by the client that contains the station ID (typically the MAC address). This is followed by an authentication response from the AP/router (WiFi gateway) containing a success or failure message. An example of when a failure may occur is if the client's MAC address is explicitly excluded in the AP/router configuration. In this mode you can enable 802.1x feature if you have another RADIUS server for user authentication. You need to input IP address, port and shared key of RADIUS server here.

▶ Authentication	Open	802.1x ☒ Enable
▶ RADIUS Server	RADIUS Server IP	0.0.0.0
	RADIUS Server Port	1812
	RADIUS Shared Key	

In this mode, you can only choose “None” or “WEP” in the encryption field.

- **Shared**

Shared key authentication relies on the fact that both stations taking part in the authentication process have the same "shared" key or passphrase. The shared key is manually set on both the client station and the AP/router. Three types of shared key authentication are available today for home or small office WLAN environments.

- **Auto**

The gateway will select appropriate authentication method according to WiFi client's request automatically.

- **WPA-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don't need additional RADIUS server for user authentication.

- **WPA2-PSK**

Select Encryption mode and enter the Pre-share Key. You can fill in 64 hexadecimal (0, 1, 2...8, 9, A, B...F) digits, or 8 to 63 ASCII characters as the pre-share key. The available encryption modes are “TKIP”, “AES”, or “TKIP/AES”. In this mode, you don't need additional RADIUS server for user authentication.

11. Scan Remote AP's MAC List: If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one. Or you can press

the “Scan” button to get the available AP’s MAC list automatically and select the expected item and copy its MAC address to the Remote AP MAC 1~4 one by one.

▶ Scan Remote AP's MAC List	Scan					
Remote AP MAC1	☒ Copy MAC to Here					
Remote AP MAC2	☐ Copy MAC to Here					
Remote AP MAC3	☐ Copy MAC to Here					
Remote AP MAC4	☐ Copy MAC to Here					
Save Undo						
Wireless AP List						
SSID	Channel	Quality	Authentication	Encryption	MAC Address	Select

12.Remote AP MAC 1 ~ Remote AP MAC 4: If you do not enable the Lazy mode, you have to enter the wireless MAC address for each WDS peer one by one.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.3.1.4 WPS Setup

Once you finished the wireless settings for the following sub-sections, you can configure and enable the WPS (Wi-Fi Protection Setup) easy setup feature for your wireless network by clicking on the “**2.4G WPS Setup**” button.

Basic Configuration [Help]	
Item	Setting
▶ Operation Band	2.4G Single Band ▼
▶ WPS	2.4G WPS Setup

2.4G Wi-Fi Protected Setup [Help]	
Item	Setting
▶ WPS	☒ Enable
▶ Configuration Status Release	CONFIGURED
▶ Configuration Mode	Registrar ▼
▶ Push-button WPS Trigger	Push-button WPS Trigger
▶ Allowed STA PIN Code	
▶ WPS Status	IDLE

- WPS¹¹:** You can enable this function by checking “Enable” box. WPS offers a safe and easy way to allow the wireless clients connected to your wireless network.
- Configuration Status:** This configuration status will be “CONFIGURED” or “UNCONFIGURED”. “CONFIGURED” means WPS connection is following WiFi settings on this gateway. If it’s released to “UNCONFIGURED”, the WPS

¹¹ Only one wireless client is allowed to proceeding WPS connection at the same time.

connection will generate a new profile.

- 3. Configuration Mode:** Select your Configuration Mode from “Registrar” or “Enrollee”. In most cases, for an AP router or AP, it should be in “Registrar” mode, so that other wireless clients in “Enrollee” mode can connect to the discovered “Registrar”. Briefly speaking, “Enrollee” is the initiator of WPS connection.

Registrar Mode

▶ Configuration Mode	Registrar ▼
▶ Push-button WPS Trigger	Push-button WPS Trigger
▶ Allowed STA PIN Code	

Enrollee Mode

▶ Configuration Mode	Enrollee ▼
▶ AP PIN Code & New Generate	00020329 New Generate

- 4. Push-button WPS Trigger [Registrar Mode]:** Press this button to simulate you have push WPS button and let wireless clients to connect to this gateway in WPS PBC mode.
- 5. Allowed STA PIN Code [Registrar Mode]:** Fill the PIN code of device, so all STA clients can operate the WPS process to the device with the certificated code.
- 6. AP PIN Code & New Generate [Enrollee Mode]:** This PIN number is required for WiFi client during WPS connection. You can press “New Generate” to get a new AP PIN.
- 7. WPS status:** According to your setting and activity, the status will show “IDLE”, “STARTPROCESS”, or “NOT USED”. The status is “IDLE” by default. If you want to start a WPS connection, you need to push “Trigger” button to change its status to “STARTPROCESS”. Only one wireless client is allowed for each WPS connection.

If you want to start a WPS connection, you can click on the “**Trigger**” button of this device to change the WPS status to “STARTPROCESS” and then initiate the WPS process on other wireless client devices in two minutes to make the client device connected to the activated WLAN.

3.1.3.2 Wireless Client List

In “**Wireless Client List**” page, the list of connected wireless clients will be shown consequently. You can choose to see “All” of connected wireless clients, or you can indicate which virtual AP (SSID) you want to browse. You can check wireless clients of VAP-1~VAP-8 individually.

Configuration Wireless Client List Advanced Configuration																				
Target WiFi [Help] <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Operation Band</td> <td>2.4G ▼</td> </tr> <tr> <td>▶ Multiple AP Names</td> <td>All ▼</td> </tr> </tbody> </table>							Item	Setting	▶ Operation Band	2.4G ▼	▶ Multiple AP Names	All ▼								
Item	Setting																			
▶ Operation Band	2.4G ▼																			
▶ Multiple AP Names	All ▼																			
Client List <table border="1"> <thead> <tr> <th>IP Address</th> <th>Host Name</th> <th>MAC Address</th> <th>Mode</th> <th>Rate</th> <th>Signal</th> <th>Interface</th> </tr> </thead> <tbody> <tr> <td colspan="7" style="text-align: center;">Refresh</td> </tr> </tbody> </table>							IP Address	Host Name	MAC Address	Mode	Rate	Signal	Interface	Refresh						
IP Address	Host Name	MAC Address	Mode	Rate	Signal	Interface														
Refresh																				

3.1.3.3 Advanced Configuration

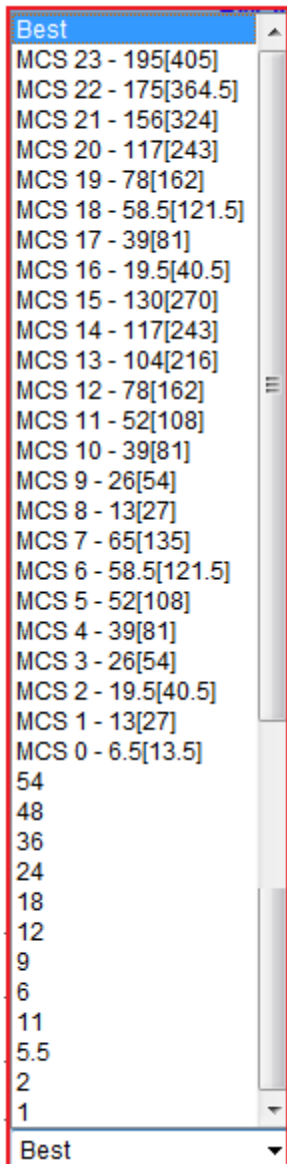
This device provides advanced wireless configuration for professional user to optimize the wireless performance under the specific installation environment.

Configuration Wireless Client List Advanced Configuration																							
Target WiFi [Help] <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Operation Band</td> <td>2.4G ▼</td> </tr> </tbody> </table>		Item	Setting	▶ Operation Band	2.4G ▼																		
Item	Setting																						
▶ Operation Band	2.4G ▼																						
Advanced Configuration <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ Regulatory Domain</td> <td>(1-13)</td> </tr> <tr> <td>▶ Beacon Interval</td> <td>100 Range: (1~1000 msec)</td> </tr> <tr> <td>▶ DTIM Interval</td> <td>3 Range: (1~255)</td> </tr> <tr> <td>▶ RTS Threshold</td> <td>2347 Range: (1~2347)</td> </tr> <tr> <td>▶ Fragmentation</td> <td>2346 Range: (256~2346)</td> </tr> <tr> <td>▶ WMM</td> <td>☒ Enable</td> </tr> <tr> <td>▶ Short GI</td> <td>400ns ▼</td> </tr> <tr> <td>▶ TX Rate</td> <td>Best ▼</td> </tr> <tr> <td>▶ RF Bandwidth</td> <td>Auto ▼</td> </tr> <tr> <td>▶ Transmit Power</td> <td>100% ▼</td> </tr> </tbody> </table>		Item	Setting	▶ Regulatory Domain	(1-13)	▶ Beacon Interval	100 Range: (1~1000 msec)	▶ DTIM Interval	3 Range: (1~255)	▶ RTS Threshold	2347 Range: (1~2347)	▶ Fragmentation	2346 Range: (256~2346)	▶ WMM	☒ Enable	▶ Short GI	400ns ▼	▶ TX Rate	Best ▼	▶ RF Bandwidth	Auto ▼	▶ Transmit Power	100% ▼
Item	Setting																						
▶ Regulatory Domain	(1-13)																						
▶ Beacon Interval	100 Range: (1~1000 msec)																						
▶ DTIM Interval	3 Range: (1~255)																						
▶ RTS Threshold	2347 Range: (1~2347)																						
▶ Fragmentation	2346 Range: (256~2346)																						
▶ WMM	☒ Enable																						
▶ Short GI	400ns ▼																						
▶ TX Rate	Best ▼																						
▶ RF Bandwidth	Auto ▼																						
▶ Transmit Power	100% ▼																						

- Operation Band:** Select the WiFi operation band that you want to configure. But the device supports only 2.4G single WiFi band.
- Regulatory Domain:** Indicate number of Wi-Fi channel. It depends on regional

government regulations.

3. **Beacon interval:** Beacons are broadcast packets that are sent by a wireless AP/router. The main purpose of beacon packet is let wireless clients know this AP (SSID) when doing wireless network scan.
4. **DTIM interval:** A DTIM is a countdown informing clients of the next window for listening to broadcast and multicast messages. When the wireless router has buffered broadcast or multicast messages for associated clients, it sends the next DTIM with a DTIM Interval value.
5. **RTS Threshold:** If an excessive number of wireless packet collision occurred, the wireless performance will be affected. It can be improved by adjusting the RTS/CTS (Request to Send/Clear to Send) threshold value.
6. **Fragmentation:** Wireless frames can be divided into smaller units (fragments) to improve performance in the presence of RF interference and at the limits of RF coverage.
7. **WMM Capable:** WMM can help control latency and jitter when transmitting multimedia content over a wireless connection.
8. **Short GI:** Time setting of Guard Interval between two Wi-Fi packets. Decrease this time interval will increase Wi-Fi data throughput. But it may cause some side-effects when the quality of Wi-Fi signal is not good. 800ns is the standard time setting of GI.
9. **TX Rate:** For WiFi transmit rate, you can choose "Best" for auto-adjustment according to WiFi signal quality in your environment, or you can fix it in certain TX rate. If you want to fix Tx rate at certain level, you need to set value of "**RF Bandwidth**" as "HT20" or "HT40" instead of "Auto". Please note the WiFi connection may be dropped if you fix at a higher data rate but in a noisy (poor RF signal quality) environment.



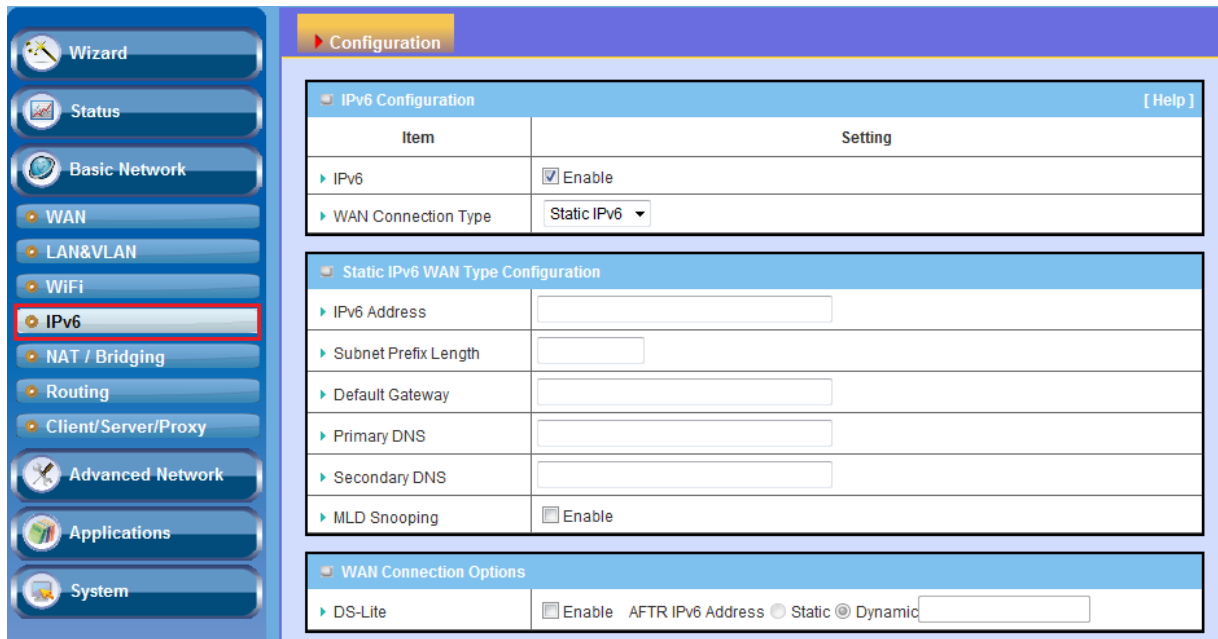
10. RF Bandwidth: Select Auto, HT20 or HT40 to define the RF bandwidth for a channel. By default, it is Auto for the device.

11. Transmit Power: Normally the wireless transmission power operates at 100% out power specification of this device. You can lower down the power ratio to prevent transmissions from reaching beyond your corporate/home office or designated wireless area.

3.1.4 IPv6 Setup

The growth of the Internet has created a need for more addresses than are possible with IPv4. **IPv6 (Internet Protocol version 6)** is a version of the Internet Protocol (IP) intended to succeed IPv4, which is the protocol currently used to direct almost all Internet traffic. IPv6 also implements additional features not present in IPv4. It

simplifies aspects of address assignment (stateless address auto-configuration), network renumbering and router announcements when changing Internet connectivity providers. This gateway supports various types of IPv6 connection (Static IPv6 / DHCPv6 / PPPoE / 6 to 4 / IPv6 in IPv4 tunnel). **Please ask your ISP of what type of IPv6 is supported before you proceed with IPv6 setup.**



IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	☒ Enable
▶ WAN Connection Type	Static IPv6 ▼

Static IPv6 WAN Type Configuration	
▶ IPv6 Address	
▶ Subnet Prefix Length	
▶ Default Gateway	
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

WAN Connection Options	
▶ DS-Lite	☐ Enable AFTR IPv6 Address ☐ Static ☒ Dynamic

3.1.4.1 Static IPv6

IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	☒ Enable
▶ WAN Connection Type	Static IPv6 ▼

When “Static IPv6” is selected for the WAN Connection Type, you need to do the following settings:

Static IPv6 WAN Type Configuration:

Static IPv6 WAN Type Configuration	
▶ IPv6 Address	
▶ Subnet Prefix Length	
▶ Default Gateway	
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

- IPv6 address:** Enter the IPv6 address here; IPv6 addresses have a size of 128 bits. Therefore, IPv6 has a vastly enlarged address space compared to IPv4. An example of an IPv6 address is
 “2001:0db8:85a3:0000:0000:8a2e:0370:7334”
- Subnet Prefix Length:** Enter the Prefix length of the Subnet Mask here; the prefix-length in IPv6 is the equivalent of the subnet mask in IPv4. However, rather than being expressed in 4 octets like it is in IPv4, it is expressed as an integer between 1 and 128. For example: 2001:db8:abcd:0012::0/64 specifies a subnet with a range of IP addresses from: 2001:db8:abcd:0012:0000:0000:0000:0000 to 2001:db8:abcd:0012:ffff:ffff:ffff:ffff.
- Default Gateway:** Enter the Default Gateway address here; a default gateway is the node on the computer network that the network software uses when an IP address does not match any other routes in the routing table.
- Primary / Secondary DNS:** You may select to obtain DNS server address automatically or use following DNS address. You may add IPv6 address Primary DNS address and secondary DNS address.
- MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

WAN Connection Options

WAN Connection Options	
▶ DS-Lite	☐ Enable AFTR IPv6 Address ☐ Static ☒ Dynamic

- DS-Lite:** If necessary in your environment, please enable this feature and enter AFTR IPv6 Address.

LAN Configuration

LAN Configuration	
▶ Global Address	/64
▶ Link-local Address	

1. **Global Address:** Please enter the global IPv6 address for LAN interface.
2. **Link-Local Address:** To show the IPv6 Link-Local address of LAN interface.

Address Auto-configuration

Address Auto-configuration	
▶ Auto-configuration	☒ Enable
▶ Auto-configuration Type	Stateless ▼
▶ Router Advertisement Lifetime	200 (seconds)

1. **Auto-configuration:** Disable or enable this auto configuration setting.
2. **Auto-configuration Type:** You may set stateless or stateful (Dynamic IPv6).
3. **Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.2 DHCP v6

IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	☒ Enable
▶ WAN Connection Type	DHCPv6 ▼

When “DHCP v6” is selected for the WAN Connection Type, you need to do the following settings:

DHCPv6 WAN Type Configuration:

DHCPv6 WAN Type Configuration	
▶ DNS	☒ From Server ☐ Specific DNS
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

1. **DNS:** You may select to obtain DNS server address from Server or entry IPv6 address Primary DNS address and secondary DNS address.
2. **MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

WAN Connection Options

WAN Connection Options	
▶ DS-Lite	☐ Enable AFTR IPv6 Address ☐ Static ☒ Dynamic

1. **DS-Lite:** If necessary in your environment, please enable this feature and enter AFTR IPv6 Address.

LAN Configuration

LAN Configuration	
▶ Global Address	
▶ Link-local Address	

1. **Global Address:** Please enter the global IPv6 address for LAN interface.
2. **Link-Local Address:** To show the IPv6 Link-Local address of LAN interface.

Address Auto-configuration

Address Auto-configuration	
▶ Auto-configuration	☒ Enable
▶ Auto-configuration Type	Stateless ▼
▶ Router Advertisement Lifetime	200 (seconds)

1. **Auto-configuration:** Disable or enable this auto configuration setting.
2. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
3. **Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces,

announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.3 PPPoEv6

IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	☒ Enable
▶ WAN Connection Type	PPPoEv6 ▼

When “PPPoEv6” is selected for the WAN Connection Type, you need to do the following settings:

PPPoEv6 WAN Type Configuration

PPPoEv6 WAN Type Configuration	
▶ Account	
▶ Password	
▶ Service Name	
▶ Connection Control	Auto-reconnect (Always on)
▶ MTU	
▶ MLD Snooping	☒ Enable

1. **Account:** enter the Username that you got from your ISP
2. **Password:** enter the Password that you got from your ISP
3. **Service Name:** enter the Service Name that you got from your ISP
4. **Connection Control:** leave the setting as “Auto-reconnect (Always on)”
5. **MTU (Maximum Transmission Unit):** Most ISP offers MTU value to users. The default MTU value is 0 (auto).
6. **MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

LAN Configuration

LAN Configuration	
▶ Global Address	
▶ Link-local Address	

1. **Global Address:** Please enter the global IPv6 address for LAN interface.
2. **Link-Local Address:** To show the IPv6 Link-Local address of LAN interface.

Address Auto-configuration

Address Auto-configuration	
▶ Auto-configuration	☒ Enable
▶ Auto-configuration Type	Stateless ▼
▶ Router Advertisement Lifetime	200 (seconds)

1. **Auto-configuration:** Disable or enable this auto configuration setting.
2. **Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
3. **Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.4 6 to 4

IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	☒ Enable
▶ WAN Connection Type	6 to 4 ▼

When “6 to 4” is selected for the WAN Connection Type, you need to do the following settings:

6to4 WAN Type Configuration

6to4 WAN Type Configuration	
▶ 6 to 4 Address	
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

- 6 to 4 Address:** You may obtain IPv6 DNS automatically or set DNS address manually for Primary DNS address and secondary DNS address.
- Primary / Secondary DNS:** Please enter IPv6 primary DNS address and secondary DNS address.
- MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

LAN Configuration

LAN Configuration	
▶ Global Address	2002:0:0: ::1
▶ Link-local Address	

- Global Address:** Please enter IPv6 global address for LAN interface.
- Link-Local Address:** To show the IPv6 Link-Local address of LAN interface.

Address Auto-configuration

Address Auto-configuration	
▶ Auto-configuration	☒ Enable
▶ Auto-configuration Type	Stateless ▼
▶ Router Advertisement Lifetime	200 (seconds)

- Auto-configuration:** Disable or enable this auto configuration setting.
- Auto-configuration type:** You may set stateless or stateful (Dynamic IPv6).
- Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the

solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.4.5 6 in 4

IPv6 Configuration [Help]	
Item	Setting
▶ IPv6	☒ Enable
▶ WAN Connection Type	6 in 4 ▼

When “6 in 4” is selected for the WAN Connection Type, you need to do the following settings:

6in4 WAN Type Configuration

6in4 WAN Type Configuration	
▶ Remote IPv4 Address	
▶ Local IPv4 Address	
▶ Local IPv6 Address	/64
▶ Primary DNS	
▶ Secondary DNS	
▶ MLD Snooping	☐ Enable

- 1. Remote / Local IPv4 and IPv6 Address:** you may add remote / local IPv4 address and local IPv6 address, then set DNS address manually for Primary DNS address and secondary DNS address.
- 2. DNS:** Please enter IPv6 primary DNS address and secondary DNS address.
- 3. MLD Snooping:** MLD snooping, IPv6 multicast data is selectively forwarded to a list of ports that want to receive the data, instead of being flooded to all ports in a VLAN. This list is constructed by snooping IPv6 multicast control packets. If necessary in your environment, please enable this feature.

LAN Configuration

LAN Configuration	
▶ Global Address	/64
▶ Link-local Address	

- 1. Global Address:** Please enter IPv6 global address for LAN interface.
- 2. Link-Local Address:** To show the IPv6 Link-Local address of LAN interface.

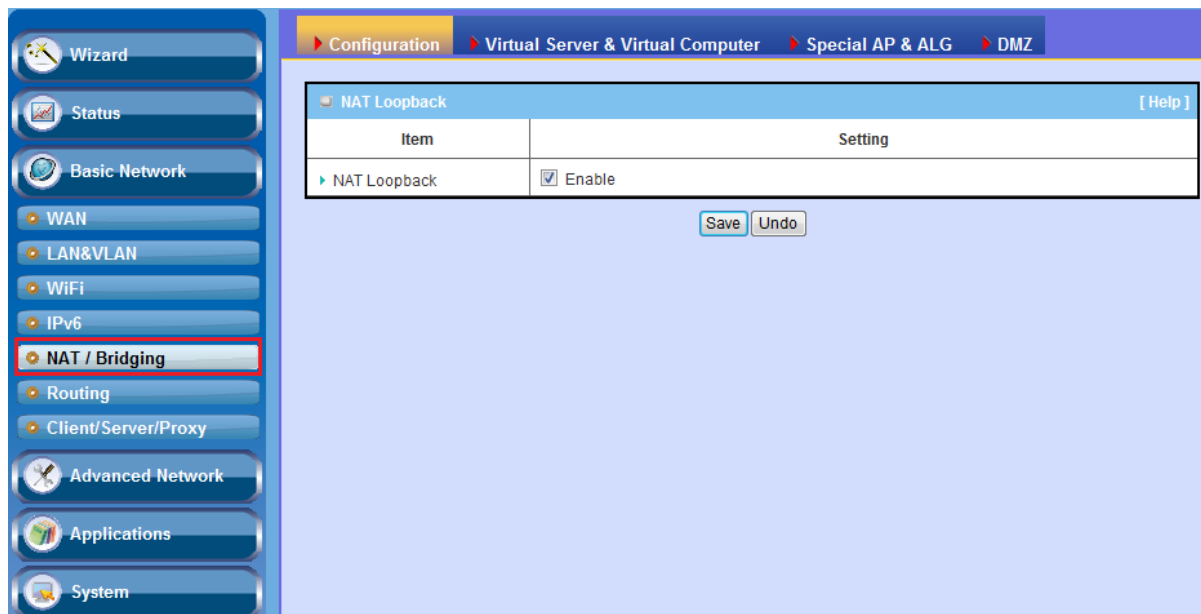
Address Auto-configuration

Address Auto-configuration	
▶ Auto-configuration	☒ Enable
▶ Auto-configuration Type	Stateless ▼
▶ Router Advertisement Lifetime	200 (seconds)

- 1. Auto-configuration:** Disable or enable this auto configuration setting.
- 2. Auto-configuration Type:** You may set stateless or stateful (Dynamic IPv6).
- 3. Router Advertisement Lifetime:** You can set the time for the period that the router send (broadcast) its router advertisement. Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address of that interface. Hosts discover the addresses of their neighboring routers simply by listening for advertisements. When a host attached to a multicast link starts up, it may multicast a Router Solicitation to ask for immediate advertisements, rather than waiting for the next periodic ones to arrive; if and only if no advertisements are forthcoming, the host may retransmit the solicitation a small number of times, but then must desist from sending any more solicitations. Any routers that subsequently start up, or that were not discovered because of packet loss or temporary link partitioning, are eventually discovered by reception of their periodic (unsolicited) advertisements.

3.1.5 NAT / Bridging

This part includes NAT related settings, such as NAT loopback, Virtual Server, Virtual Computer, Special AP, ALG, and DMZ.



NAT Loopback	
Item	Setting
▶ NAT Loopback	☒ Enable

Save Undo

3.1.5.1 Configuration

NAT Loopback [Help]	
Item	Setting
▶ NAT Loopback	☒ Enable

1. **NAT Loopback:** Allow you to access the WAN IP address from inside your local network. This is useful when you run a server inside your network. For an example, if you set a mail server at LAN side, your local devices can access this mail server through gateway's WAN IP address. You don't need to change IP address of mail server no matter you are at local side or go out. This is useful when you run a server inside your network.

3.1.5.2 Virtual Server & Virtual Computer

3.1.5.2.1 Virtual Server

Virtual Server List Add Delete							
ID	Public Port	Server IP	Private Port	Protocol	Time Schedule	Enable	Actions

This gateway's NAT firewall filters out unrecognized packets to protect your Intranet, so all hosts behind this device are invisible to the outside world. If you wish, you can make some of them accessible by enabling the Virtual Server Mapping. Press "Add" button to add new rule for Virtual Server.

A virtual server is defined as a **Public Port**, and all requests to this port will be redirected to the computer specified by the **Server IP**. Virtual Server can work with **Scheduling Rules**, and give user more flexibility on Access control. For the details, please refer to **System->Scheduling**.

Virtual Server Rule Configuration	
Item	Setting
▶ Public Port	User-defined Service
▶ Server IP	
▶ Private Port	
▶ Protocol	Both
▶ Time Schedule	Always
▶ Rule	☐ Enable

For example, if you have an **FTP server (Service port 21)** at **192.168.123.1**, a **Web server1 (Service port 80)** at **192.168.123.2**, a **Web server2 (Service Port 8080)** and

Private port 80) at 192.168.123.3, and a VPN server at 192.168.123.6, then you need to specify the following virtual server mapping table

Public Port	Server IP	Private Port	Protocol	Rule
21	192.168.123.1		TCP	Enable
80	192.168.123.2		TCP	Enable
8080	192.168.123.3	80	TCP	Enable
1723	192.168.123.6		Both	Enable

3.1.5.2.2 Virtual Computer

Virtual Computer enables you to use the original NAT feature, and allows you to setup the one-to-one mapping of multiple global IP address and local IP address. Press “Add” button to add new rule for Virtual Computer.

Virtual Computer List
Add
Delete

ID	Global IP	Local IP	Enable	Actions
----	-----------	----------	--------	---------

Virtual Computer Rule Configuration
[Help]

Global IP	Local IP	Enable
		☐

Save

1. **Global IP:** Enter the global IP address assigned by your ISP.
2. **Local IP:** Enter the local IP address of your LAN PC corresponding to the global IP address.
3. **Enable:** Check this item to enable the Virtual Computer feature.

3.1.5.2.3 Special AP & ALG

NAT feature can protect Intranet from outside attacks, but sometimes also blocks some applications, such as SIP VoIP. In this situation, the NAT gateway needs to do special process (ALG) for each application. This gateway can handle SIP ALG, so you need to enable this option if you want to use SIP applications at LAN side of this gateway.

Configuration

Item	Setting
▶ ALG	SIP ALG ☒ Enable

Some applications require multiple connections, like Internet games, Video

conferencing, Internet telephony, etc. Because of the firewall function, these applications cannot work with a pure NAT router. **The Special Applications** feature allows some of these applications to work with this product. If the mechanism of Special Applications fails to make an application work, try setting your computer as the DMZ host instead.

Special AP List Add Delete					
ID	Trigger Port	Incoming Ports	Time Schedule	Enable	Actions

Press “Add” button to add new rule for Special AP.

Special AP Rule Configuration [Help]	
Item	Setting
▶ Trigger Port	Port : Popular Applications : -- select one -- ▼
▶ Incoming Ports	
▶ Time Schedule	(0) Always ▼
▶ Rule	☐
Save	

This device provides some predefined settings. Select your application item, and all related settings will be filled up automatically.

1. **Trigger Port:** The outbound port number issued by the application.
2. **Incoming Ports:** When the trigger packet is detected, the inbound packets sent to the specified port numbers are allowed to pass through the firewall.
3. **Time Schedule:** Each special AP setting can be turned off according to the schedule rule you specified. By default, it is always turned on when the rule is enabled.
4. **Rule:** Check this item to enable the Special AP rule.

3.1.5.3 DMZ

Configuration [Help]	
Item	Setting
▶ IP Address of DMZ Host	☐ Enable
▶ Relay	DHCP Relay ☐ 192.168.123.254

DMZ (DeMilitarized Zone) Host is a host without the protection of firewall. It allows a computer to be exposed to unrestricted 2-way communication for Internet games, Video conferencing, Internet telephony and other special applications. Otherwise, if

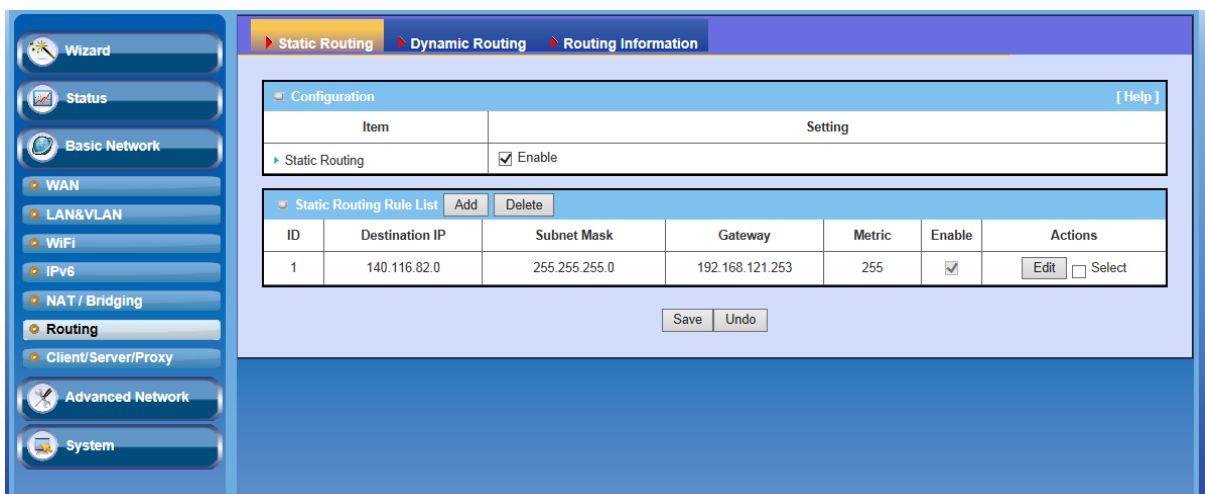
specific application is blocked by NAT mechanism, you can indicate that LAN computer as a DMZ host to solve this problem.

- 1. IP Address of DMZ Host:** Enter IP address of Server or Host.
- 2. DHCP Relay:** DHCP Relay Agent component relays DHCP messages between DHCP clients and DHCP servers on different IP networks. Because DHCP is a broadcast-based protocol, by default its packets do not pass through routers. If you need this feature in the environment, please enable it.

NOTE: This feature should be used only when needed.

3.1.6 Routing Setup

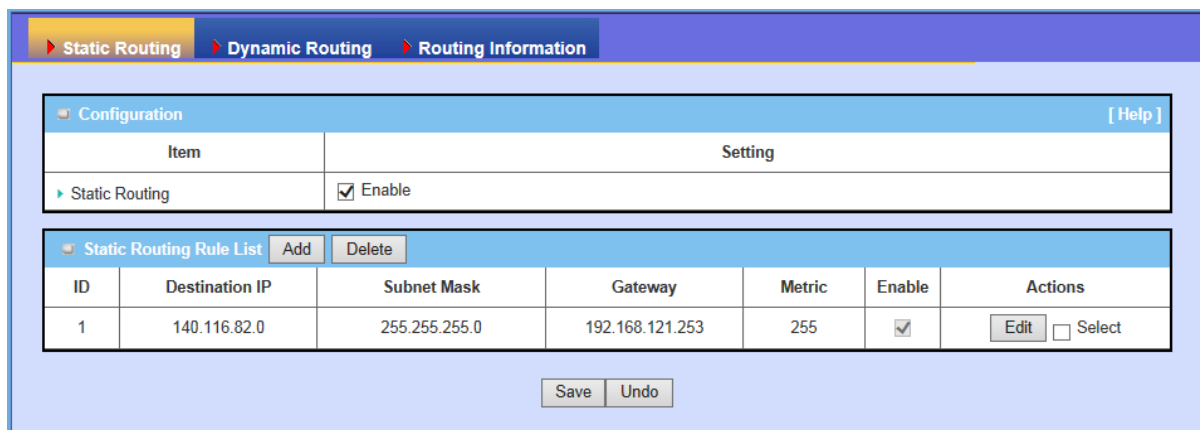
If you have more than one router and subnet, you will need to enable routing function to allow packets to find proper routing path and allow different subnets to communicate with each other.



Configuration							[Help]
Item	Setting						
Static Routing	☒ Enable						

Static Routing Rule List							Add	Delete
ID	Destination IP	Subnet Mask	Gateway	Metric	Enable	Actions		
1	140.116.82.0	255.255.255.0	192.168.121.253	255	☒	Edit Select		

3.1.6.1 Static Routing



Configuration							[Help]
Item	Setting						
Static Routing	☒ Enable						

Static Routing Rule List							Add	Delete
ID	Destination IP	Subnet Mask	Gateway	Metric	Enable	Actions		
1	140.116.82.0	255.255.255.0	192.168.121.253	255	☒	Edit Select		

For static routing, you can specify up to 32 routing rules. The routing rules allow you

to determine which physical interface addresses are utilized for outgoing IP data grams. You can enter the **destination IP address**, **Subnet Mask**, **Gateway**, and **Metric** for each routing rule, and then enable or disable the rule by checking or un-checking the Enable checkbox.

Please click Add or Edit button to configure a static routing rule:

Static Routing Rule Configuration	
Item	Setting
▶ Destination IP	140.116.82.0
▶ Subnet Mask	255.255.255.0
▶ Gateway IP	192.168.121.253
▶ Metric	255
▶ Rule	☒ Enable

1. **Destination IP:** Enter the subnet network of routed destination.
2. **Subnet Mask:** Input your subnet mask. Subnet mask defines the range of IP address in destination network.
3. **Gateway:** The IP address of gateway that you want to route for this destination subnet network. The assigned gateway is required to be in the same subnet of LAN side or WAN side.
4. **Metric:** The router uses the value to determine the best possible route. It will go in the direction of the gateway with the lowest metric.
5. **Rule:** Check the Enable box to enable this static routing rule.

3.1.6.2 Dynamic Routing

The feature of static route is for you to maintain routing table manually. In addition, this gateway also supports dynamic routing protocol, such as RIPv1/RIPv2, OSPF, BGP for you to establish routing table automatically. The feature of dynamic routing will be very useful when there are lots of subnets in your network. Generally speaking, RIP is suitable for small network. OSPF is more suitable for medium network. BGP is more used for big network infrastructure.

Static Routing
Dynamic Routing
Routing Information

RIP Configuration [Help]

Item	Setting
RIP	Disable

OSPF Configuration

Item	Setting
OSPF	☐ Enable
Backbone Subnet	

OSPF Area List Add Delete

ID	Area Subnet	Area ID	Enable	Actions
----	-------------	---------	--------	---------

BGP Configuration

Item	Setting
BGP	☐ Enable
Self ID	

BGP Neighbor List Add Delete

ID	Neighbor IP	Neighbor ID	Enable	Actions
----	-------------	-------------	--------	---------

- RIP:** Routing Information Protocol (RIP) will exchange information about destinations for computing routes throughout the network. Please select RIPv2 only if you have different subnets in your network. Otherwise, please select RIPv1 if you need this protocol.
- OSPF:** OSPF is an interior gateway protocol that routes Internet Protocol (IP) packets solely within a single routing domain (autonomous system). It gathers link state information from available routers and constructs a topology map of the network. The topology determines the routing table presented to the Internet Layer which makes routing decisions based solely on the destination IP address found in IP packets.

OSPF Configuration				
Item	Setting			
OSPF	☒ Enable			
Backbone Subnet	192.168.10.0/24			

OSPF Area List Add Delete				
ID	Area Subnet	Area ID	Enable	Actions
1	192.168.101.0/24	192.168.101.1	☒	Edit ☐ Select
2	192.168.102.0/24	192.168.102.1	☒	Edit ☐ Select
3	192.168.103.0/24	192.168.103.1	☒	Edit ☐ Select

OSPF Area Configuration	
Item	Setting
Area Subnet	192.168.103.0/24
Area ID	192.168.103.1
Area	☒ Enable

Save

You can enable the OSPF routing function by checking “Enable” checkbox for the OSPF item and filling the “Backbone Subnet”. You can add up to 8 area subnets for the OSPF network and enable them individually. But also you can modify some existed OSPF areas by clicking corresponding “Edit” command buttons at the end of each OSPF area definition in the OSPF Area List. Besides, unnecessary OSPF areas can be removed by checking the “Select” box for those areas and then clicking on the “Delete” command button at the OSPF Area List caption. When you finished setting, click on **“Save”** to store your settings.

- BGP:** Border Gateway Protocol (BGP) is the protocol backing the core routing decisions on the Internet. It maintains a table of IP networks or 'prefixes' which designate network reach-ability among autonomous systems (AS). It is described as a path vector protocol. BGP does not use traditional Interior Gateway Protocol (IGP) metrics, but makes routing decisions based on path, network policies and/or rule-sets. For this reason, it is more appropriately termed a reach-ability protocol rather than routing protocol.

BGP Configuration	
Item	Setting
BGP	☒ Enable
Self ID	10100

BGP Neighbor List Add Delete				
ID	Neighbor IP	Neighbor ID	Enable	Actions
1	192.168.101.1	101	☒	Edit ☐ Select
2	192.168.102.1	102	☒	Edit ☐ Select
3	192.168.103.1	103	☒	Edit ☐ Select

bgp Area Configuration	
Item	Setting
Neighbor IP	192.168.103.1
Neighbor ID	103
Neighbor	☒ Enable
Save	

You can enable the BGP routing function by checking “Enable” checkbox for the BGP item and filling the “Self ID”. You can add up to 8 BGP neighbors for the BGP network and enable them individually. But also you can modify some existed BGP neighbors by clicking corresponding “Edit” command buttons at the end of each BGP neighbor definition in the BGP Neighbor List. Besides, unnecessary BGP neighbors can be removed by checking the “Select” box for those neighbors and then clicking on the “Delete” command button at the BGP Neighbor List caption. When you finished setting, click on “**Save**” to store your settings.

3.1.6.3 Routing Information

Static Routing Dynamic Routing Routing Information				
Routing Information				
Destination	Gateway	Subnet Mask	Metric	Interface
192.168.76.0	192.168.121.253	255.255.255.0	0	WAN-1
140.116.82.0	192.168.121.253	255.255.255.0	255	WAN-1
192.168.121.0	0.0.0.0	255.255.255.0	0	WAN-1
192.168.75.0	0.0.0.0	255.255.255.0	0	LAN
140.116.0.0	0.0.0.0	255.255.0.0	0	WAN-1
239.0.0.0	0.0.0.0	255.0.0.0	0	LAN
127.0.0.0	0.0.0.0	255.0.0.0	0	lo
0.0.0.0	192.168.121.253	0.0.0.0	0	WAN-1

A routing table, or routing information base (RIB), is a data table stored in a router or a networked computer that lists the routes to particular network destinations, and in some cases, metrics (distances) associated with those routes. The routing table contains information about the topology of the network immediately around it.

This page displays the routing table maintained by this device. It is generated

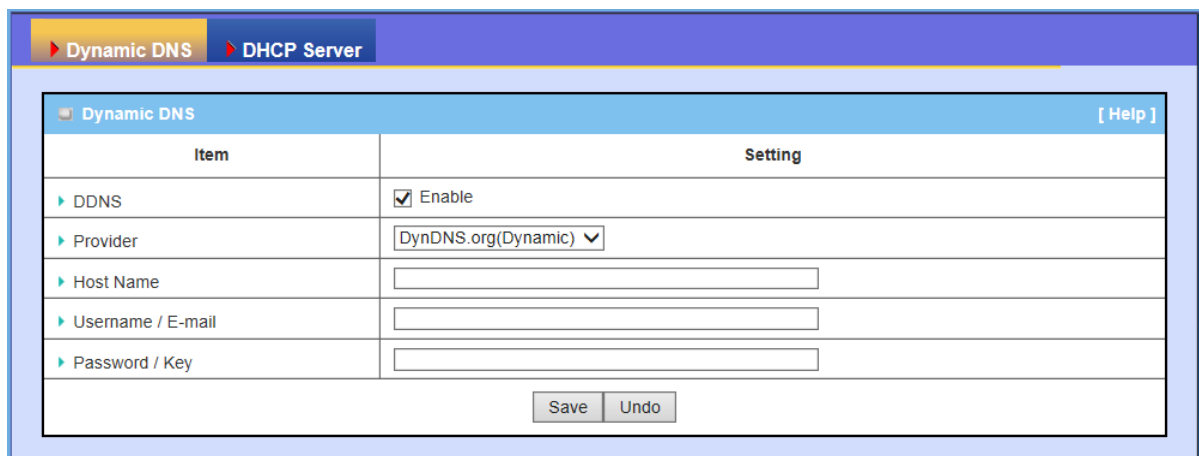
according to your network configuration.

3.1.7 Client/Server/Proxy

3.1.7.1 Dynamic DNS

For remote access to the GEM420 4G router via 3G/4G network connection to use port forwarding to connect to devices on the LAN and you are not using Fixed IP SIM card services then there is the option of using a DDNS service provider. It can be free or charged. For 3G/4G connection your service provider will need to provide public IP address and this is not available from all providers so you will need to check.

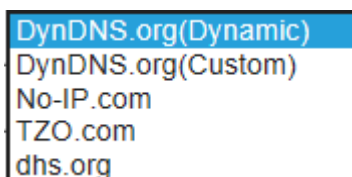
To host your server on a changing IP address, you have to use dynamic domain name service (DDNS). Therefore, anyone wishing to reach your host only needs to know the name of it. Dynamic DNS will map the name of your host to your current IP address, which changes each time you connect your Internet service provider. This device supports most popular 3-party DDNS service provider, including TZO.com, No-IP.com, DynDNS.org(Dynamic), DynDNS.org(Custom), and DHS.org. Before you enable **Dynamic DNS**, you need to register an account on one of these Dynamic DNS servers that we list in **Provider** field.



Item	Setting
▶ DDNS	☒ Enable
▶ Provider	DynDNS.org(Dynamic) ▼
▶ Host Name	
▶ Username / E-mail	
▶ Password / Key	

Save Undo

1. **DDNS:** Check the Enable box if you would like to activate this function.
2. **Provider:** The DDNS provider supports service for you to bind your IP (even private IP) with a certain Domain name. You could choose your favorite provider. There are following options:



DynDNS.org(Dynamic)
 DynDNS.org(Custom)
 No-IP.com
 TZO.com
 dhs.org

3. **Host Name:** Register a domain name to the DDNS provider. The fully domain name is concatenated with hostname (you specify) and a suffix(DDNS provider specifies).
4. **Username/E-mail:** Input username or E-mail based on the DDNS provider you registered.
5. **Password/Key:** Input password or key based on the DDNS provider you select.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.1.7.2 DHCP Server

The gateway supports up to 4 DHCP servers to serve the DHCP requests from different VLAN groups and DMZ port. And there is one default one whose LAN IP Address and Subnet Mask are the same ones of gateway LAN interface, and IP Pool ranges from .100 to .200 as shown at following DHCP Server List. You can add or edit one DHCP server configuration by clicking on the “Add” button behind “DHCP Server List” or the “Edit” button at the end of DHCP server information.

There is additional button can be used to do fix mapping between MAC address and IP address of local client hosts as following diagram.

Dynamic DNS

DHCP Server

DHCP Server List

Add

Delete

DHCP Server Name	LAN IP Address	Subnet Mask	IP Pool	Lease Time	Domain Name	Primary DNS	Secondary DNS	Primary WINS	Secondary WINS	Gateway	Server Enable	Actions
DHCP 1	192.168.123.254	255.255.255.0	192.168.123.100-192.168.123.200	86400		0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	0.0.0.0	☒	Edit

Fixed Mapping...

DHCP Server Configuration

Press “Add” button to add a new DHCP server profile or press “Edit” button to modify profile of existed DHCP server.

DHCP Server Configuration	
Item	Setting
▶ DHCP Server Name	DHCP 2
▶ LAN IP Address	
▶ Subnet Mask	255.0.0.0 (/8)
▶ IP Pool	Starting Address: Ending Address:
▶ Lease Time	86400 seconds
▶ Domain Name	
▶ Primary DNS	
▶ Secondary DNS	
▶ Primary WINS	
▶ Secondary WINS	
▶ Gateway	
▶ Server	☒ Enable

- DHCP Server Name:** The server name of DHCP server. By default, they are "DHCP 1" ~ "DHCP 4".
- LAN IP Address:** Specify the local IP address of the enabled DHCP Server. It's the LAN IP address of this gateway for DHCP server. For other DHCP servers, their LAN IP Addresses also have default values and can be modifies by user.
- Subnet Mask:** Select the subnet mask for the specific DHCP-n server. Subnet Mask defines how many clients are allowed in one network or subnet. It is the same to the one of LAN interface for DHCP-1 server. For other DHCP servers, the default subnet mask is 255.255.255.0/24, and it means maximum 254 IP addresses are allowed in this subnet. However, one of them is occupied by LAN IP address of this gateway, so there are maximum 253 clients allowed in LAN network. Hereafter are the available options for subnet mask.

255.0.0.0 (/8)
255.128.0.0 (/9)
255.192.0.0 (/10)
255.224.0.0 (/11)
255.240.0.0 (/12)
255.248.0.0 (/13)
255.252.0.0 (/14)
255.254.0.0 (/15)
255.255.0.0 (/16)
255.255.128.0 (/17)
255.255.192.0 (/18)
255.255.224.0 (/19)
255.255.240.0 (/20)
255.255.248.0 (/21)
255.255.252.0 (/22)
255.255.254.0 (/23)
255.255.255.0 (/24)
255.255.255.128 (/25)
255.255.255.192 (/26)
255.255.255.224 (/27)
255.255.255.240 (/28)
255.255.255.248 (/29)
255.255.255.252 (/30)

4. **IP Pool Starting / Ending Address:** Whenever there is a request, the DHCP server will automatically allocate an unused IP address from the IP address pool to the requesting computer. You must specify the starting / ending address of the IP address pool. Please note the number of IP address in this IP pool must less than the maximum number of subnet network that according to the subnet mask you set.
5. **Lease Time:** DHCP lease time to the DHCP client.
6. **Domain Name:** Optional, this information will be passed to the clients.
7. **Primary DNS/Secondary DNS:** Optional. This feature allows you to assign DNS Servers.
8. **Primary WINS/Secondary WINS:** Optional. This feature allows you to assign WINS Servers.
9. **Gateway:** Optional. Gateway address would be the IP address of an alternate Gateway. This function enables you to assign another gateway to your local computer when DHCP server offers IP address. For an example, this gateway will assign IP address to local computers, but local computers will go to Internet through another gateway.
10. **Server:** Check the "Enable" box to activate the DHCP server.

Fixed Mapping

Press "**Fixed Mapping ...**" button at the bottom of the DHCP server list page and you can specify a certain IP address for designated local device (MAC address) by manual, so that the DHCP Server will reserve the special IPs for designated devices.

For internal servers, you can use this feature to ensure each of them receives same IP address all the time.

Fixed Mapping

[Help]

DHCP clients

-- select one --

Copy to

 ID

--

ID	MAC Address	IP Address	Enable
1			☐
2			☐
3			☐
4			☐
5			☐
6			☐
7			☐
8			☐
9			☐
10			☐

<<Previous

Next>>

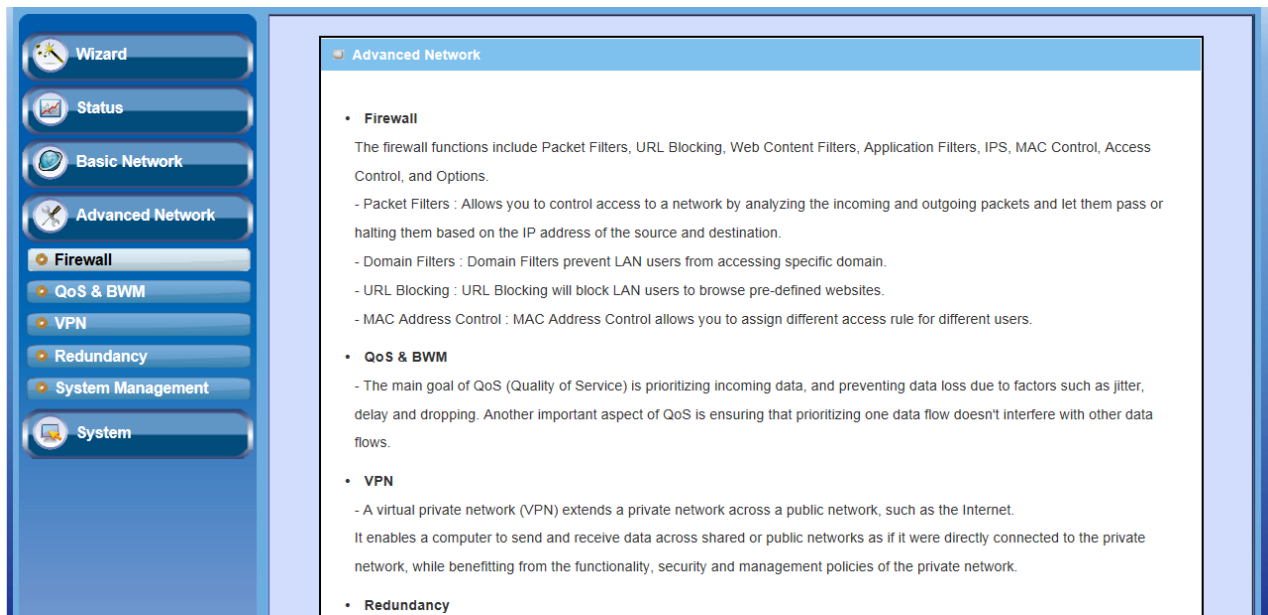
Save

Undo

Back

3.2 Advanced Network

This device also supports many advanced network features, such as Firewall, QoS & Bandwidth Management, VPN Security, Redundancy and System Management. You can finish those configurations in this section.

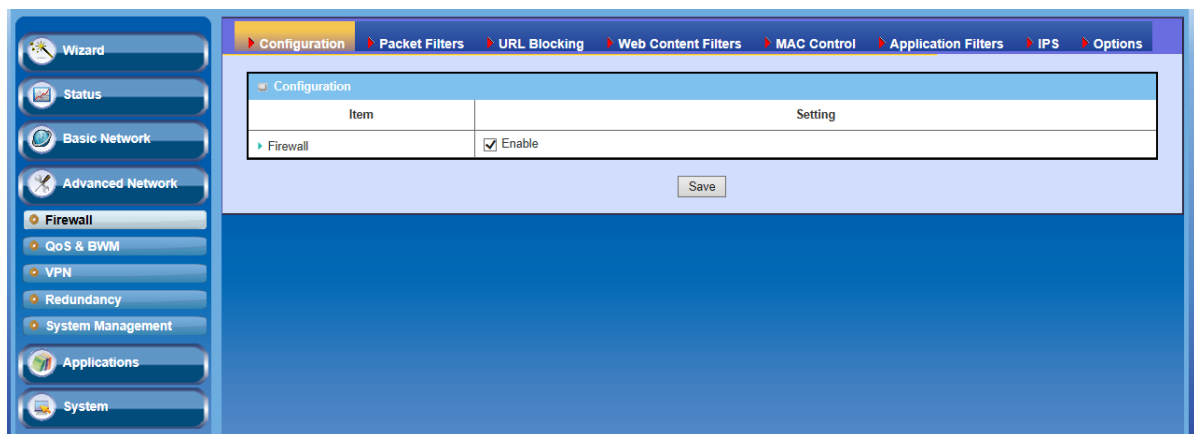


3.2.1 Firewall

The firewall functions include Packet Filters, URL Blocking, Web Content Filters, MAC Control, Application Filters, IPS and some firewall options.

3.2.1.1 Configuration

One Firewall Enable check box lets you activate all firewall functions that you want.



3.2.1.2 Packet Filters

Packet Filters function can let you define both outbound filter and inbound filter rules by specifying the source IP and destination IP in a rule. It enables you to control what packets are allowed or blocked to pass the router. Outbound filters are applied to all outbound packets. However, inbound filters are applied to packets that destined to virtual servers or DMZ host / port only.

Configuration Packet Filters URL Blocking Web Content Filters MAC Control Application Filters IPS Options

Configuration [Help]

Item	Setting
Packet Filters	☒ Enable
Black List / White List	Allow all to pass except those match the following rules. ▼
Log Alert	☐ Enable

Packet Filter List Add Delete

ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Destination Port	Protocol	Time Schedule	Enable	Actions
1	Block 75.2 Telnet	Any	Any	192.168.75.2	0.0.0.0	23-23	Both	(0) Always	☒	Edit Select

Save Undo MAC Level

3.2.1.2.1 Configuration

You can enable packet filter function here. And select one of the two filtering policies as follows. The first one is to define the black list. System will block the packets that match the active filter rules. However, the second one is the white list. System will allow the packets to pass the gateway, which match the active filter rules.

1. Allow all to pass except those match the specified rules. (Black List)
2. Deny all to pass except those match the specified rules. (White List)

Configuration [Help]

Item	Setting
Packet Filters	☒ Enable
Black List / White List	Allow all to pass except those match the following rules. ▼
Log Alert	☐ Enable

Besides, you also can enable the log alerting so that system will record packet blocking events when filter rules are fired. At the right upper corner of screen, one "[Help]" command let you see the on-line help message about Packet Filter function.

3.2.1.2.2 Packet Filter List

It is a list of all packet filter rules. You can add one new rule by clicking on the "Add" command button. But also you can modify some existed packet filter rules by clicking corresponding "Edit" command buttons at the end of each filter rule in the Packet Filter List. Besides, unnecessary rules can be removed by checking the "Select" box for those rules and then clicking on the "Delete" command button at the Packet Filter List caption.

Packet Filter List Add Delete										
ID	Rule Name	From Interface	To Interface	Source IP	Destination IP	Destination Port	Protocol	Time Schedule	Enable	Actions
1	Block 75.2 Telnet	Any	Any	192.168.75.2	0.0.0.0	23-23	Both	(0) Always	☒	Edit ☐ Select

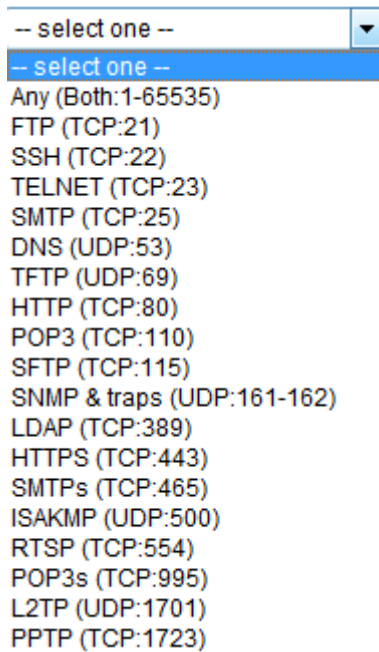
3.2.1.2.3 Packet Filter Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one packet filter rule. They are Rule Name, From Interface, To Interface, Source IP, Destination IP, Destination Port, Protocol, Time Schedule and finally, the rule enable.

Packet Filter Rule Configuration	
Item	Setting
▶ Rule Name	Block 75.2 Telnet
▶ From Interface	Any
▶ To Interface	Any
▶ Source IP	Specific IP Address 192.168.75.2
▶ Destination IP	Specific IP Address 0.0.0.0
▶ Destination Port	User-defined Service 23 - 23
▶ Protocol	Both
▶ Time Schedule	(0) Always
▶ Rule	☒ Enable

Save Undo Back

- Rule Name:** The name of packet filter rule.
- From Interface:** Any interface or someone LAN interface or someone WAN interface.
- To Interface:** Any interface or someone LAN interface or someone WAN interface.
- Source IP:** Specify the Source IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A "0.0.0.0" implies all IP addresses.
- Destination IP:** Specify the Destination IP address of packets that want to be filtered out in the packet filter rule. You can define a single IP address (4.3.2.1) or a range of IP addresses (4.3.2.20~30). A "0.0.0.0" implies all IP addresses.
- Destination Port:** Choose "User-defined Service" to let you specify manually the destination service port of packets that want to be filtered out in the packet filter rule. You can define a single port (80) or a range of ports (1000-1999). A "0" implies all ports are used. You also can choose one well-known service instead so that the chosen service will provide its destination port and protocol number for the rule. The supported well-known services include:



7. **Protocol:** Specify which packet protocol is to be filtered. It can be TCP, UDP, or Both.
8. **Time Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.
9. **Rule Enable:** Check the enable box if you want to activate the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “**Save**” to store your settings or click “**Undo**” to give up the changes.

3.2.1.3 URL Blocking

URL Blocking will block the webs containing pre-defined key words. This feature can filter both domain input suffix (like .com or .org, etc) and a keyword “bct” or “mpe”.

Configuration Packet Filters **URL Blocking** Web Content Filters MAC Control Application Filters IPS Options

Configuration [Help]

Item	Setting
▶ URL Blocking	☒ Enable
▶ Black List / White List	Allow all to pass except those match the following rules. ▼
▶ Log Alert	☒ Enable
▶ Invalid Access Web Redirection	☒ Enable

URL Blocking Rule List Add Delete

ID	Rule Name	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions
1	anti-gaming	gaming	0	(0) Always	☒	Edit ☐ Select

Save Undo

3.2.1.3.1 Configuration

Configuration [Help]

Item	Setting
▶ URL Blocking	☒ Enable
▶ Black List / White List	Allow all to pass except those match the following rules. ▼
▶ Log Alert	☒ Enable
▶ Invalid Access Web Redirection	☒ Enable

- URL Blocking:** Check the enable box if you want to activate URL Blocking function.
- Black List / White List:** Select one of the two filtering policies for the defined rules in URL Blocking Rule List.
 - Allow all to pass except those match the specified rules (Black List).
 - Deny all to pass except those match the specified rules (White List).
- Log Alert:** Enable the log alerting so that system will record URL blocking events when blocking rules are fired.
- Invalid Access Web Redirection:** Users will see a specific web page to know their access is blocked by rules.
- [Help]:** At the right upper corner of screen, one “[Help]” command let you see the on-line help message about URL Blocking function.

3.2.1.3.2 URL Blocking Rule List

It is a list of all URL Blocking rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed URL blocking rules by clicking corresponding “Edit” command buttons at the end of each blocking rule in the URL Blocking Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the URL Blocking Rule List caption.

URL Blocking Rule List Add Delete						
ID	Rule Name	URL / Domain Name / Keyword	Destination Port	Time Schedule	Enable	Actions
1	anti-gaming	gaming		(0) Always	☒	Edit ☐ Select

3.2.1.3.3 URL Blocking Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one URL blocking rule. They are Rule Name, URL / Domain Name / Keyword, Destination Port, Time Schedule and finally, the rule enable.

URL Blocking Rule Configuration	
Item	Setting
▶ Rule Name	anti-gaming
▶ URL / Domain Name / Keyword	gaming
▶ Destination Port	-
▶ Time Schedule	(0) Always ▼
▶ Rule	☒ Enable

Save Undo Back

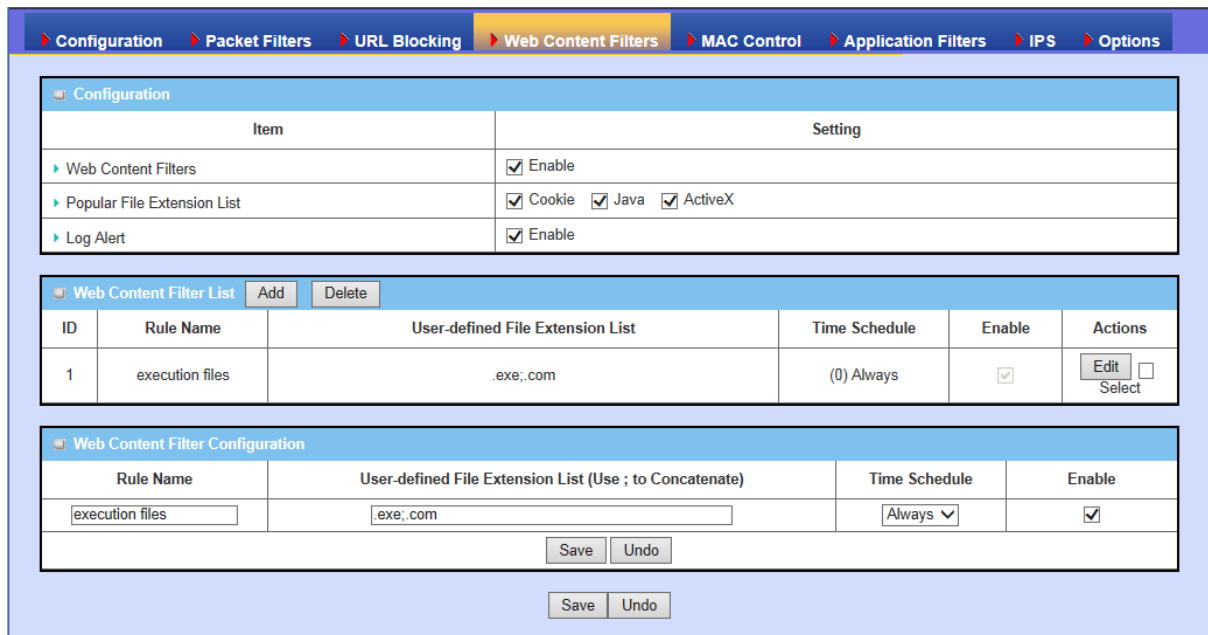
- Rule Name:** The name of URL blocking rule.
- URL/Domain Name/Keyword:** If any part of the Website's URL matches the pre-defined words, the connection will be blocked. You can enter up to 10 pre-defined words in a rule and each URL keyword is separated by ",", e.g., "google, yahoo, org"; In addition to URL keywords, it can also block the designated domain name, like "www.xxx.com", "www.123aaa.org, mma.com".
- Destination Port:** Specify the destination port in URL requests that want to be blocked in the URL blocking rule. You can define a single port (80) or a range of ports (1000-1999). An empty or "0" implies all ports are used.
- Time Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.
- Rule Enable:** Check the enable box if you want to activate the rule. Each rule can be enabled or disabled individually.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

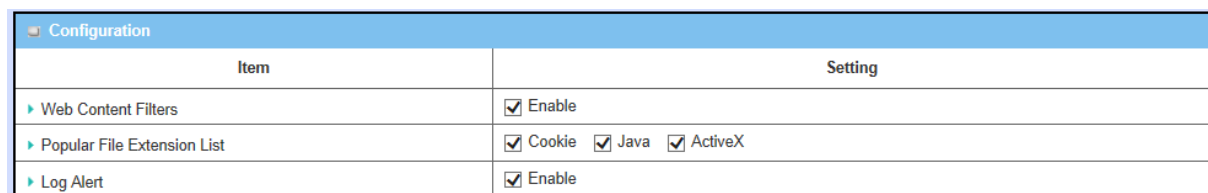
3.2.1.4 Web Content Filters

Web Content Filters can block HTML requests with the specific extension file name,

like ".exe", ".bat" (applications), "mpeg" (video), and block HTML requests with some script types, like Java Applet, Java Scripts, cookies and Active X.



3.2.1.4.1 Configuration



- 1. Web Content Filters:** Check the Enable box if you want to enable Web Content Filters function.
- 2. Popular File Extension List:** Check which extension types, Cookie, Java, ActiveX, are to be blocked.
- 3. Log Alert:** Enable the log alerting so that system will record Web content filtering events when filtering rules are fired.

3.2.1.4.2 Web Content Filter Rule List

It is a list of all Web Content Filter rules. You can add one new rule by clicking on the "Add" command button. But also you can modify some existed Web Content Filter rules by clicking corresponding "Edit" command buttons at the end of each filtering rule in the Web Content Filter List. Besides, unnecessary rules can be removed by checking the "Select" box for those rules and then clicking on the "Delete" command button at the Web Content Filter List caption.

Web Content Filter List Add Delete					
ID	Rule Name	User-defined File Extension List	Time Schedule	Enable	Actions
1	execution files	.exe;.com	(0) Always	☒	Edit ☐ Select

3.2.1.4.3 Web Content Filter Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one Web Content Filter rule. They are Rule Name, User-defined File Extension List, Time Schedule and finally, the rule enable.

Web Content Filter Configuration			
Rule Name	User-defined File Extension List (Use ; to Concatenate)	Time Schedule	Enable
execution files	.exe;.com	Always	☒
Save Undo			

- Rule Name:** The name of Web Content Filter rule.
- User-defined File Extension List:** You can enter up to 10 file extensions to be blocked in a rule by using ';' to concatenate these file extensions.
- Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** -> **Scheduling** menu.
- Enable:** Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.1.5 MAC Control

MAC Control allows you to assign different access right for different users based on device's MAC address.

Configuration Packet Filters URL Blocking Web Content Filters **MAC Control** Application Filters IPS Options

Configuration [Help]

Item	Setting
MAC Control	☒ Enable
Black List / White List	Allow all to pass except those match the following rules. ▾
Log Alert	☒ Enable
Known MAC from LAN PC List	-- select one -- ▾ Copy to

MAC Control Rule List Add Delete

ID	Rule Name	MAC Address	Time Schedule	Enable	Actions
1	Block JP NB	20:6A:6A:6A:6B	(0) Always	☒	Edit ☐ Select

MAC Control Rule Configuration

Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Block JP NB	20:6A:6A:6A:6B	Always ▾	☒

Save Undo

Save Undo

Saved!

3.2.1.5.1 Configuration

Configuration [Help]

Item	Setting
MAC Control	☒ Enable
Black List / White List	Allow all to pass except those match the following rules. ▾
Log Alert	☒ Enable
Known MAC from LAN PC List	-- select one -- ▾ Copy to

- MAC Control:** Check the “Enable” box to activate the MAC Control function. All of the settings in this page will take effect only when “Enable” is checked.
- Black List / White List:** Select one of the two filtering policies for the defined rules.
 Black List - Allow all to pass except those match the specified rules.
 White List - Deny all to pass except those match the specified rules
- Log Alert:** Enable the log alerting so that system will record MAC control events when control rules are fired.
- Known MAC from LAN PC List:** You can see all of connected clients from this list, and copy their MAC address to the MAC Control Rule Configuration window below.

3.2.1.5.2 MAC Control Rule List

It is a list of all MAC Control rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed MAC control rules by clicking corresponding “Edit” command buttons at the end of each control rule in the MAC

Control Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the MAC Control Rule List caption.

MAC Control Rule List Add Delete					
ID	Rule Name	MAC Address	Time Schedule	Enable	Actions
1	Block JP NB	20:6A:6A:6A:6A:6B	(0) Always	☒	Edit ☐ Select

3.2.1.5.3 MAC Control Rule Configuration

It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one MAC Control rule. They are Rule Name, MAC Address, Time Schedule and finally, the rule enable.

MAC Control Rule Configuration			
Rule Name	MAC Address (Use : to Compose)	Time Schedule	Enable
Block JP NB	20:6A:6A:6A:6A:6B	Always	☒
Save Undo			

- Rule Name:** The name of Web Content Filter rule.
- MAC Address:** Input the MAC address of local device. You can input manually or copy it from **Known MAC from LAN PC List**. Please note the format of MAC address is like “xx:xx:xx:xx:xx:xx”. “x” is a hexadecimal digit.
- Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System -> Scheduling** menu.
- Enable:** Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

3.2.1.6 Application Filters

Application Filters can categorize Internet Protocol packets based on their application layer data and allow or deny their passing of gateway.

This device supports the application filters for various Internet chat software, P2P download, Proxy, and A/V streaming. You can select the applications to be blocked after the function is enabled, and specify the schedule rule for such Application Filters function.

Configuration	
Item	Setting
Application Filters	☒ Enable
Log Alert	☒ Enable
Schedule	(0) Always ▾

Chat Software	
QQ	☒ Enable
Facebook	☒ Enable
Skype	☒ Enable
Aliww	☒ Enable

P2P Software	
BT(BitTorrent, BitSpirit, BitComet)	☒ Enable
eDonkey/eMule/Shareaza	☒ Enable
HTTP Multiple Thread Download	☒ Enable

3.2.1.6.1 Configuration

Configuration	
Item	Setting
Application Filters	☒ Enable
Log Alert	☒ Enable
Schedule	(0) Always ▾

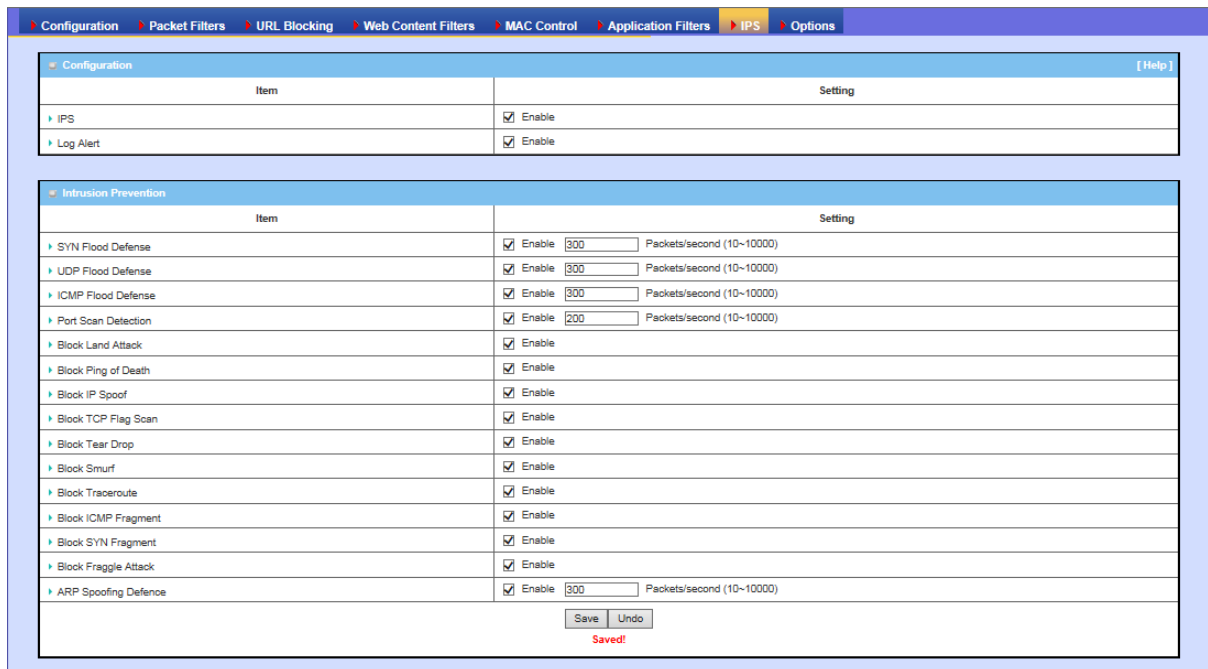
- Application Filters:** Check the “Enable” box to activate the Application Filters function. All of the settings in this page will take effect only when “Enable” is checked.
- Log Alert:** Enable the log alerting so that system will record Application Filter events when filtering rules are fired.
- Schedule:** All Application Filter rules can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, they are always turned on when Application Filters function is enabled. For more details, please refer to the **System -> Scheduling** menu.

3.2.1.7 IPS

IPS (Intrusion Prevention Systems) are network security appliances that monitor network and/or system activities for malicious activity. The main functions of IPS are to identify malicious activity, log information about this activity, attempt to block/stop it and report it.

You can enable the IPS function and check the listed intrusion activities if necessary. There are some intrusion prevention items need a further Threshold parameter to work properly for intrusion detection. Besides, you can enable the log alerting so that

system will record Intrusion events when corresponding intrusions are detected.



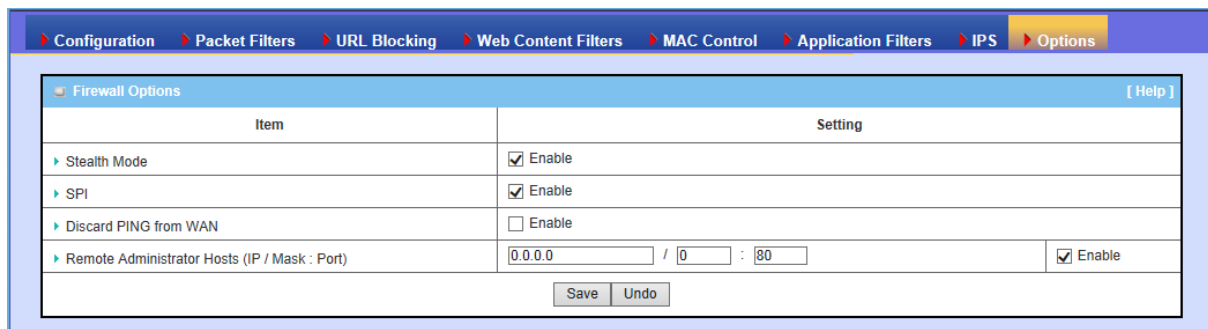
Item	Setting
IPS	☒ Enable
Log Alert	☒ Enable

Item	Setting
SYN Flood Defense	☒ Enable 300 Packets/second (10~10000)
UDP Flood Defense	☒ Enable 300 Packets/second (10~10000)
ICMP Flood Defense	☒ Enable 300 Packets/second (10~10000)
Port Scan Detection	☒ Enable 200 Packets/second (10~10000)
Block Land Attack	☒ Enable
Block Ping of Death	☒ Enable
Block IP Spoof	☒ Enable
Block TCP Flag Scan	☒ Enable
Block Tear Drop	☒ Enable
Block Smurf	☒ Enable
Block Traceroute	☒ Enable
Block ICMP Fragment	☒ Enable
Block SYN Fragment	☒ Enable
Block Fraggle Attack	☒ Enable
ARP Spoofing Defence	☒ Enable 300 Packets/second (10~10000)

Save Undo

Saved!

3.2.1.8 Options



Item	Setting
Stealth Mode	☒ Enable
SPI	☒ Enable
Discard PING from WAN	☐ Enable
Remote Administrator Hosts (IP / Mask : Port)	0.0.0.0 / 0 : 80 ☒ Enable

Save Undo

- Stealth Mode:** Enable this feature, this device will not respond to port scans from the WAN so that makes it less susceptible to discovery and attacks on the Internet.
- SPI:** When this feature is enabled, the router will record the outgoing packet information pass through the router like IP address, port address, ACK, SEQ number and so on. And the router will check every incoming packet to detect if this packet is valid.
- Discard PING from WAN:** If this feature is enabled, this gateway won't reply any ICMP request packet from WAN side. It means any remote host can't get response when "ping" to this gateway. "Ping" is a useful command that we use to detect if a certain host is alive or not. But it also let hacker know about this. Therefore, many Internet servers will be set to ignore IGMP request.
- Remote Administrator Hosts (IP / Mask : Port):** In general, only local clients

(LAN users) can browse the device's built-in web pages for device administration setting. This feature enables you to perform administration task from a certain remote host. If this feature is enabled, only the specified IP address can perform remote administration. If the specified IP address is 0.0.0.0, any host can connect with this product to perform administration task. You can use subnet mask bits "/nn" notation to specified a group of trusted IP addresses. For example, "10.1.2.0/24".

NOTE: When Remote Administration is enabled, the web server port will be configured to 80 as default. You also can change web server port to other port

Afterwards, click on "Save" to store your settings or click "Undo" to give up the changes.

3.2.2 QoS & BWM

The total amount of data traffic increases nowadays as the higher demand of mobile devices, like Game / Chat / VoIP / P2P / Video / Web access. In order to pose new requirements for data transport, e.g. low latency, low data loss, the entire network must ensure them via a connection service guarantee.

The main goal of QoS & BWM (Quality of Service and Bandwidth Management) is prioritizing incoming data, and preventing data loss due to factors such as jitter, delay and dropping. Another important aspect of QoS is ensuring that prioritizing one data flow doesn't interfere with other data flows. So, QoS helps to prioritize data as it enters your router. By attaching special identification marks or headers to incoming packets, QoS determines which queue the packets enter, based on priority. This is useful when there are certain types of data you want to give higher priority to, such as voice packets given higher priority than Web data packets.

To utilize your network throughput completely, administrator must define bandwidth control rules carefully to balance the utilization of network bandwidth for all users to access. It is indeed required that an access gateway satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management. PROROUTE Security Gateway provides a Rule-based QoS to carry out the requirements.

- Wizard
- Status
- Basic Network
- Advanced Network
- Firewall
- QoS & BWM**
- VPN
- Redundancy
- System Management
- Applications
- System

Configuration
Rule-based QoS

System Resource Configuration [Help]

Item	Setting
▶ Total Priority Queues of All WANs	
▶ WAN Interface	WAN - 1

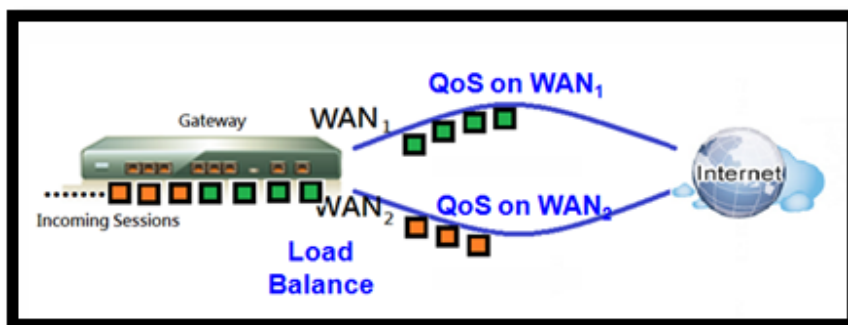
WAN Interface Resource

Item	Setting
▶ Bandwidth of Upstream	0 Mbps
▶ Bandwidth of Downstream	0 Mbps
▶ Total Connection Sessions	
▶ Flexible Bandwidth Management	☐ Enable

3.2.2.1 Configuration

■ QoS on Multiple WAN Interfaces

- QoS on all WAN interfaces satisfies the requirements of latency-critical applications, minimum access right guarantee, fair bandwidth usage for same subscribed condition and flexible bandwidth management in a more flexible approach.
- Integrated with Multi-WAN load balance function to maximize the total network throughput.



■ Flexible Bandwidth Management (FBM)

- Adjust the bandwidth distribution dynamically based on current bandwidth usage situation to get the maximum system network performance, and it is transparent to all users.

Before QoS & BWM function can work correctly, this gateway needs to define the resource for each WAN interface. First one is the available bandwidth of WAN connection. It was set in the **Basic Network -> WAN -> Physical Interface** menu and shown here. Second one is the maximum number of connection sessions that the WAN interface supports. The last is the maximum number of priority queues that the WAN interface supports.

Configuration Rule-based QoS	
System Resource Configuration [Help]	
Item	Setting
Total Priority Queues of All WANs	
WAN Interface	WAN - 1 ▼
WAN Interface Resource	
Item	Setting
Bandwidth of Upstream	0 Mbps ▼
Bandwidth of Downstream	0 Mbps ▼
Total Connection Sessions	
Flexible Bandwidth Management	☐ Enable

- Total Priority Queues of All WANs:** Input the maximum number of priority queues for all WAN interfaces.
- WAN Interface:** Select the WAN interface to configure following parameters.
- Bandwidth of Upstream:** The maximum bandwidth of uplink in Mbps.
- Bandwidth of Downstream:** The maximum bandwidth of downlink in Mbps.
- Total Connection Sessions:** Input the maximum number of connection sessions for the WAN interface.

3.2.2.2 Rule-based QoS

This gateway provides lots of flexible rules for you to set QoS policies. Basically, you need to know three parts of information before you create your own policies. First, “who” needs to be managed? Second, “what” kind of service needs to be managed? The last part is “how” you prioritize. Once you get this information, you can continue to learn more details in this section.

■ Flexible QoS Rule Definition

- Multiple Group Categories
 - Specify the group category in a QoS rule for the target objects that rule to be applied on.
 - Group Category can bases on VLAN ID, MAC Address, IP Address, Host Name or Packet Length. Category depends on model.
- Differentiated Services
 - Specify the service type in a QoS rule for the target packets that rule to be applied on.
 - Differentiated services can be base on 802.1p, DSCP, TOS, VLAN ID, User-defined Services and Well-known Services.

- Well-known services include FTP(21), SSH(TCP:22), Telnet(23), SMTP(25), DNS(53), TFTP(UDP:69), HTTP(TCP:80), POP3(110), Auth(113), SFTP(TCP:115), SNMP&Traps(UDP:161-162), LDAP(TCP:389), HTTPS(TCP:443), SMTPs(TCP:465), ISAKMP(500), RTSP(TCP:554), POP3s(TCP:995), NetMeeting(1720), L2TP(UDP:1701) and PPTP(TCP:1723).
- Available Control Functions
 - There are 4 resources can be applied in a QoS rule: bandwidth, connection sessions, priority queues and DiffServ Code Point (DSCP). Control function that acts on target objects for specific services of packet flow is based on these resources.
 - For bandwidth resource, control functions include guaranteeing bandwidth and limiting bandwidth. For priority queue resource, control function is setting priority. For DSCP resource, control function is DSCP marking. The last resource is Connection Sessions; the related control function is limiting connection sessions.
- Individual / Group Control
 - One QoS rule can be applied to individual member or whole group in the target group. This feature depends on model.
- Outbound / Inbound Control
 - One QoS rule can be applied to the outbound or inbound direction of packet flow, even them both. This feature depends on model.

3.2.2.2.1 Configuration

It supports the activation of Rule-based QoS.

Configuration [Help]	
Item	Setting
▶ Rule-based Qos Enable	☒ Enable

1. **Rule-based QoS Enable:** Check the box if you want to enable the QoS & BWM function.

Besides, at the right upper corner of screen, one “[Help]” command let you see the on-line help message about Rule-based QoS function.

3.2.2.2.2 QoS Rule List

It is a list of all QoS rules. You can add one new rule by clicking on the “Add” command button. But also you can modify some existed QoS rules by clicking

corresponding “Edit” command buttons at the end of each rule in the QoS Rule List. Besides, unnecessary rules can be removed by checking the “Select” box for those rules and then clicking on the “Delete” command button at the QoS Rule List caption. One “Clear” command button can let you clear all rules and “Restart” command button can let you restart the operation of all QoS rules.

QoS Rule List									
Add Delete Clear Restart									
Interface	Group	Service	Resource	Control Function	Direction	Sharing Method	Time Schedule	Enable	Actions
All WANs	20:6A:6A:6A:6A:B6	ALL	Bandwidth	10-10	Inbound	Group	(0) Always	☒	Edit ☐ Select
Save Undo									

- Add:** After you enabled the rule-based QoS function, you can click on the “Add” button to create a new QoS rule.
- Delete:** After you selected some QoS rules by checking the “Select” box for each rule, you can click on the “Delete” button to remove those rules from the list.
- Clear:** Delete all existed QoS rules.
- Restart:** Press “Restart” button to re-initiate all QoS rules again.
- Edit:** Configure the specific QoS rule again.

3.2.2.2.3 QoS Rule Configuration

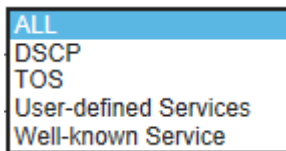
It supports the adding of one new rule or the editing of one existed rule. There are some parameters need to be specified in one QoS rule. They are Interface, Group, Service, Resource, Control Function, QoS Direction, Sharing Method, Time Schedule and finally, the rule enable.

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs ▼
▶ Group	Src. MAC Address ▼
▶ Service	ALL ▼
▶ Resource	Bandwidth ▼
▶ Control Function	Set MINR & MAXR ▼ --- Mbps ▼
▶ QoS Direction	Outbound ▼
▶ Sharing Method	Group Control ▼
▶ Time Schedule	(0) Always ▼
▶ Rule	☐ Enable

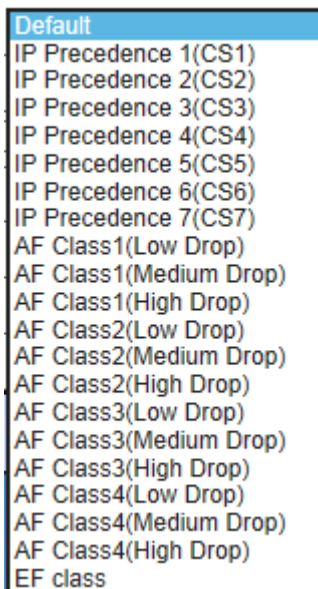
- Interface:** Select the WAN interface for the QoS rule.
- Group:** Specify the target client members for the rule by their VLAN ID, MAC Address, IP Address, Host Name or Group Object. “IP Address” group can be

defined as an IP range. And “Group Object” is defined in the **System -> Grouping** menu. But what kinds of groups to use depend on model.

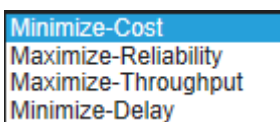
3. **Service:** There are 5 options for service, including All, DSCP, TOS, User-defined Services and Well-known Service, like



By default, it is “All”. It defines “what” kinds of service packets need to be managed. When “DSCP” is selected, another “DiffServ CodePoint” value must be specified. DSCP means DiffServ Code Point, as known as advanced TOS. You can choose this option if your local service gateway supports DSCP tags. The DSCP categories that this gateway can detect are as below.



You need to choose a correct one according to your device's specification. When “TOS” is selected for Service, TOS value must be chosen from a list of 4 options. For example:



When “User-defined Services” is selected, two more parameters, Protocol Number and Service Port Range, must be defined. Protocol Number is either TCP or UDP or Both. Finally, when “Well-known Service” is selected, you can choose the well-known from a list like:

Any(Both 1-65535)
FTP(21)
SSH(TCP:22)
Telnet(23)
SMTP(25)
DNS(53)
TFTP(UDP:69)
HTTP(TCP:80)
POP3(110)
Auth(113)
SFTP(TCP:115)
SNMP&Traps(UDP:161-162)
LDAP(TCP:389)
HTTPS(TCP:443)
SMTPs(TCP:465)
ISAKMP(500)
RTSP(TCP:554)
POP3s(TCP:995)
NetMeeting(1720)
L2TP(UDP:1701)
PPTP(TCP:1723)

4. **Resource:** There are 4 resources can be chosen to control in a QoS rule. They are “Bandwidth”, “Connection Sessions”, “Priority Queues” and “DiffServ Code Points”.
5. **Control Function:** It depends on the chosen resource. For “Bandwidth” resource, the control function is “Set MINR & MAXR”. For “Connection Sessions”, the control function is “Set Session Limitation”. For “Priority Queues”, it is “Set Priority”. However, for “DiffServ Code Points”, it is “DSCP Marking” and you need specify the DSCP value additionally.
6. **QoS Direction:** Select the traffic direction to be applied for this rule.

Direction	
IN	For Inbound data
OUT	For Outbound data
BOTH	Inbound and Outbound

7. **Sharing Method:** If you want to apply the value of control setting on each selected host in the “Group”, you need to select “Individual Control” for Sharing Method. On the other hand, if the value of control setting wants to be applied on all selected hosts in the “Group”, you need to select “Group Control”. For example, you define Control Function as “Set Session Limitation” and the limited sessions are 2000 sessions. You also define Sharing Method as “Individual Control”. Then, that means the maximum connection sessions of each selected host can’t exceed 2000 sessions. On the contrary, changing to “Group Control”, it means that group of client hosts totally can’t use over 2000 connection sessions.
8. **Schedule:** The rule can be turn on according to the schedule rule you specified, and give user more flexibility on access control. By default, it is always turned on when the rule is enabled. For more details, please refer to the **System** ->

Scheduling menu.

9. **Enable:** Check the box if you want to enable the rule. Each rule can be enabled or disabled individually.

Afterwards, click on “Save” to store your settings or click “Undo” to give up the changes.

Example #1 for adding a “DSCP” type QoS rule

QoS Rule Configuration	
Item	Setting
▶ Interface	All WANs ▼
▶ Group	IP ▼ 192.168.75.10 -- 40
▶ Service	DSCP ▼ ▶ DiffServ CodePoint IP Precedence 4(CS4) ▼
▶ Resource	DiffServ Code Points ▼
▶ Control Function	DSCP Marking ▼ AF Class2(High Drop) ▼
▶ QoS Direction	Inbound ▼
▶ Sharing Method	Group Control ▼
▶ Time Schedule	(0) Always ▼
▶ Rule	☒ Enable

- ◆ Interface: Select “All WANs”.
- ◆ Group: Select “IP” and enter IP range: 192.168.75.10 ~ 40.
- ◆ Service: Select “DSCP” with DiffServ CodePoint is CS4.
- ◆ Resource: Select “DiffServ Code Points”.
- ◆ Control Function: Select “DSCP Marking” with “AF Class 2(High Drop)”.
- ◆ QoS Direction: Select “Inbound” for inbound traffic only.
- ◆ Sharing Method: Select “Group Control”.
- ◆ Schedule: Leave the default value of “(0) Always” as it is.

This rule means IP packets from all WAN interfaces to LAN IP address 192.168.75.10 ~ 192.168.75.40 which have DiffServ code points with “IP Precedence 4(CS4)” value will be modified by “DSCP Marking” control function with “AF Class 2(High Drop)” value at any time.

Example #2 for adding a “Connection Sessions” type QoS rule

QoS Rule Configuration	
Item	Setting
▶ Interface	WAN - 1 ▼
▶ Group	IP ▼ 192.168.75.10 -- 40
▶ Service	ALL ▼
▶ Resource	Connection Sessions ▼
▶ Control Function	Set Session Limitation ▼ 20000
▶ QoS Direction	Outbound ▼
▶ Sharing Method	Group Control ▼
▶ Time Schedule	(0) Always ▼
▶ Rule	☒ Enable

- ◆ Interface: Select “WAN-1”.
- ◆ Group: Select “IP” and enter IP range: 192.168.75.10 ~ 40.
- ◆ Service: Select “ALL”.
- ◆ Resource: Select “Connection Sessions”.
- ◆ Control Function: Select “Set Session Limitation”, and set session number to 20000.
- ◆ QoS Direction: Select “Outbound” for outbound traffic only. It is for the client devices under the gateway to establish multiple sessions with servers in the Internet.
- ◆ Sharing Method: Select “Group Control”.
- ◆ Schedule: Leave the default value of “(0) Always” as it is.

This rule defines that all client hosts, whose IP address is in the range of 192.168.75.10~40, can access to the Internet and keep a maximum 20000 connection sessions totally at any time.

3.2.3 VPN Setup

A virtual private network (VPN) extends a private network across a public network, such as the Internet. It enables a computer to send and receive data across shared or public networks as if it were directly connected to the private network, while benefitting from the functionality, security and management policies of the private network. This is done by establishing a virtual point-to-point connection through the use of dedicated connections, encryption, or a combination of the two. The tunnel technology supports data confidentiality, data origin authentication and data integrity of network information by utilizing encapsulation protocols, encryption algorithms, and hashing algorithms.

The product series supports following tunneling technologies to establish secure tunnels between multiple sites for data transferring, including IPSec, PPTP, L2TP (over IPSec) and GRE. Advanced functions include Full Tunnel, Tunnel Failover, Tunnel Load Balance,

NetBIOS over IPSec, NAT Traversal and Dynamic VPN.

In Configuration page, there is only one parameter, “VPN” with “Enable” checkbox. Check that box to activate the VPN function whatever you use which tunneling technology beforehand.



3.2.3.1 IPSec

Internet Protocol Security (IPSec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPSec includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session.

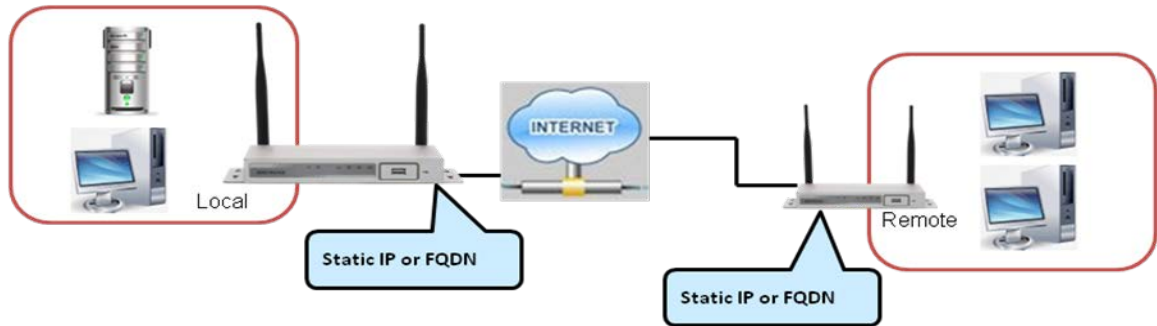
An IPSec VPN tunnel is established between IPSec client and server. Sometimes, we call the IPSec VPN client as the initiator and the IPSec VPN server as the responder. There are two phases to negotiate between the initiator and responder during tunnel establishment, IKE phase and IPSec phase. At IKE phase, IKE authenticates IPSec peers and negotiates IKE SAs (Security Association) during this phase, setting up a secure channel for negotiating IPSec SAs in phase 2. At IPSec phase, IKE negotiates IPSec SA parameters and sets up matching IPSec SAs in the peers. After these both phases, data is transferred between IPSec peers based on the IPSec parameters and keys stored in the SA database.

3.2.3.1.1 IPSec VPN Tunnel Scenarios

There are some common IPSec VPN connection scenarios as follows:

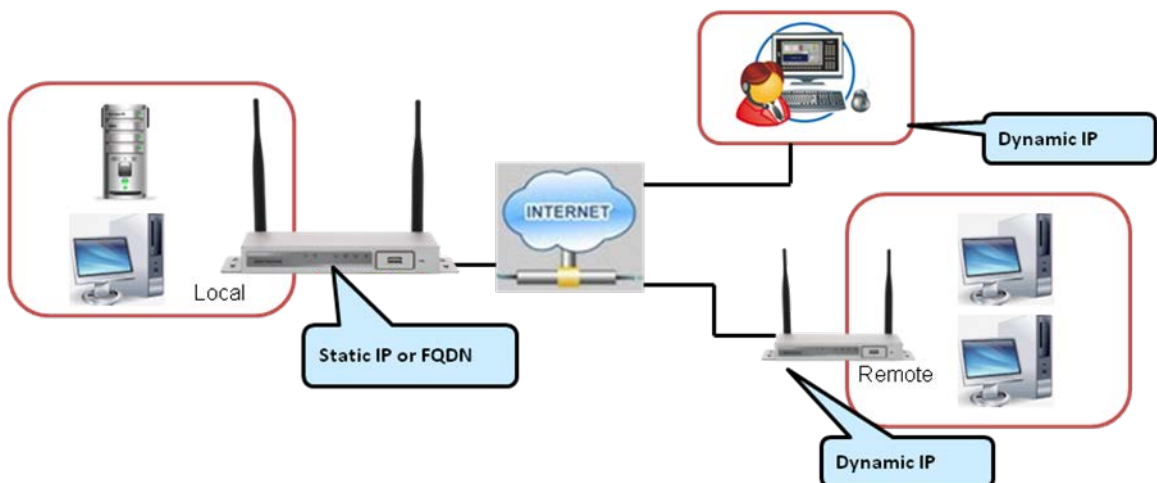
- Site to Site

The device establishes IPSec VPN tunnels with security gateway in headquarters or branch offices. Either local or remote peer gateway which can be recognized by a static IP address or a FQDN can initiate the establishing of an IPSec VPN tunnel. Two peers of the tunnel have their own Intranets and the secure tunnel serves for data communication between these two subnets of hosts.



- **Dynamic VPN**

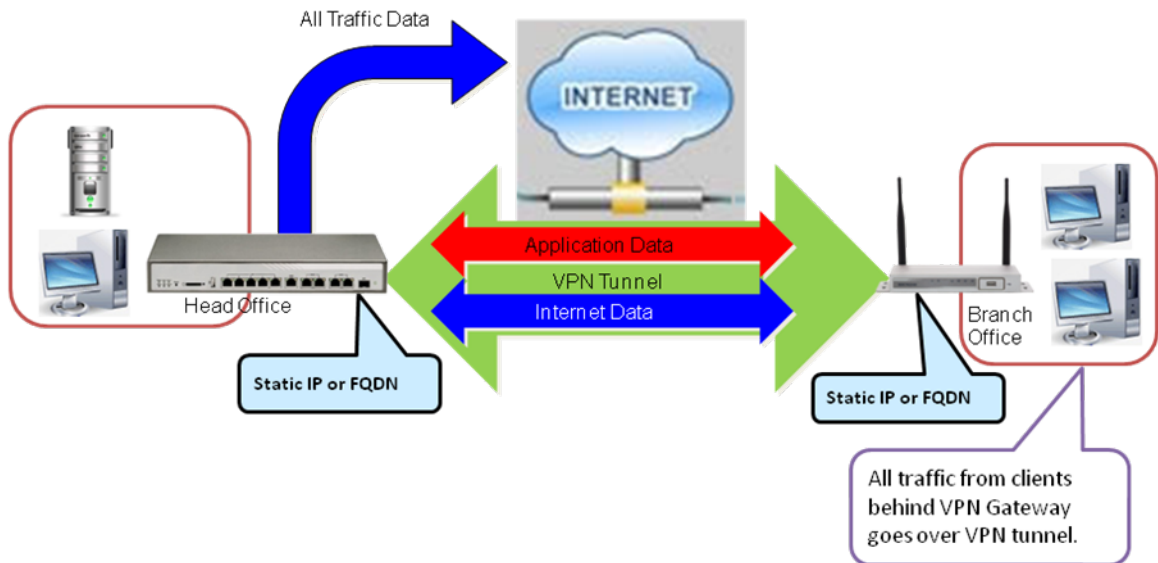
Business Security Gateway can ignore IP information of clients when using Dynamic VPN, so it is suitable for users to build VPN tunnels with Business Security Gateway from a remote mobile host or mobile site. Remote peer is a host or a site will be indicated in the negotiation packets, including what remote subnet is. It must be noted that the remote peer has to initiate the tunnel establishing process first in this application scenario.



There is one more advanced IPsec VPN application:

- **Site to Site – Support Full Tunnel Application**

When Full Tunnel function of remote Business Security Gateway is enabled, all data traffic from remote clients behind remote Business Security Gateway will go over the VPN tunnel. That is, if a user is operating at a PC that is in the Intranet of remote Business Security Gateway, all application packets and private data packets from the PC will be transmitted securely in the VPN tunnel to access the resources behind local Business Security Gateway, including surfing the Internet. As a result, every time the user surfs the web for shopping or searching data on Internet, checking personal emails, or accessing company servers, all are done in a secure way through local Business Security Gateway.



3.2.3.1.2 IPSec Configuration

Configuration [HELP]	
Item	Setting
▶ IPSec	☐ Enable
▶ NetBIOS over IPSec	☐ Enable
▶ NAT Traversal	☐ Enable
▶ Max. Tunnels	32

1. **IPSec:** You could trigger the function of IPSec VPN if you check “Enable” box.
2. **NetBIOS over IPSec:** If you would like two Intranets behind two Business Security Gateways to receive the NetBIOS packets from Network Neighborhood, you have to check “Enable” box.
3. **NAT Traversal:** Some NAT routers will block IPSec packets if they don’t support IPSec pass through. If your Business Security Gateway connects to this kind of NAT router which doesn’t support IPSec pass through, you need to activate this option in your Business Security Gateway.
4. **Max. Tunnels:** The device supports up to 32 IPSec tunnels, but you can specify it with the number of maximum current activated IPSec tunnels that is smaller or equal to 32.
5. You can add new, edit or delete some IPSec tunnels in Tunnel List & Status as follows.

3.2.3.1.3 Tunnel List & Status

Tunnel List & Status Add Delete Refresh							
ID	Interface	Tunnel Name	Remote Address	Gateway	Status	Enable	Actions
1	WAN 1	MyDynamicVPN	Any	Any	On	☒	Edit ☐ Select
2	WAN 1	IPSec_Site2Site	10.0.76.0/ 255.255.255.0	www.ipsec_site2site.com.tw		☒	Edit ☐ Select

1. **Add:** You can add one new IPSec tunnel with Site to Site scenario by clicking the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking the “Delete” button.
3. **Refresh:** To refresh the Tunnel List & Status each 2 seconds by clicking on the “Refresh” button.
4. **Tunnel:** Check the “Enable” box to activate the IPSec tunnel.
5. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

3.2.3.1.4 Local & Remote Configuration

Local & Remote Configuration	
Item	Setting
▶ Local Subnet	10.0.75.0
▶ Local Netmask	255.255.255.0 -- select one -- -- select one -- -- select one -- -- select one --
▶ Full Tunnel	☐ Enable
▶ Remote Subnet	10.0.76.0
▶ Remote Netmask	255.255.255.0 -- select one -- -- select one -- -- select one -- -- select one --
▶ Remote Gateway	www.ipsec_site2site.com.tw (IP Address/FQDN)

1. **Local Subnet:** The subnet of LAN site of local Business Security Gateway. It can be a host, a partial subnet, the whole subnet or multiple subnets of LAN site of local gateway. The device supports VPN hub and spoke function. There are 5 local subnets to be defined here and the information will be transferred to remote VPN sites for routing remote packets to these 5 local subnets via this VPN tunnel.
2. **Local Netmask:** The local netmask and associated local subnet IP can define a subnet domain for the local devices connected via the VPN tunnel. There are 5 local subnet domains to be defined here for hub and spoke function.

3. **Full Tunnel:** All traffic from Intranet of Business Security Gateway goes over the IPSec VPN tunnel if these packets don't match the Remote Subnet of other IPSec tunnels. That is, both application data and Internet access packets land up at the VPN concentrator.
4. **Remote subnet:** The subnet of LAN site of remote Business Security Gateway. It can be a host, a partial subnet, the whole subnet or multiple subnets of LAN site of remote gateway. Since the device supports VPN hub and spoke function, there are 5 remote subnets to be defined here and any packets want to these 5 remote subnets will be transferred via this VPN tunnel.
5. **Remote Netmask:** The remote netmask and associated remote subnet IP can define a subnet domain for the remote devices connected via the VPN tunnel. There are 5 remote subnet domains to be defined here for hub and spoke function.
6. **Remote Gateway:** Enter the IP address or FQDN of remote Business Security Gateway.

3.2.3.1.6 Authentication

Authentication	
Item	Setting
▶ Key Management	IKE+Pre-shared Key ▼ 12345678 (Min. 8 characters)
▶ Local ID	Type: Username ▼ ID:
▶ Remote ID	Type: Username ▼ ID:

1. **Key Management:** Select "IKE+Pre-shared Key" or "Manually". Other options depend on product models. By default, "IKE+Pre-shared Key" method is adopted for key management. It is the first key used in IKE phase for both VPN tunnel initiator and responder to negotiate further security keys to be used in IPSec phase. The pre-shared key must be the same for both VPN tunnel initiator and responder. When "Manually" key management is adopted, the Pre-shared is not necessary.
2. **Local ID:** The Type and the Value of the local Business Security Gateway must be the same as that of the Remote ID of the remote VPN peer. There are 4 types for Local ID: User Name, FQDN, User@FQDN and Key ID.
3. **Remote ID:** The Type and the Value of the local Business Security Gateway must be the same as that of the local ID of the remote VPN peer. There are also 4 types for Remote ID: User Name, FQDN, User@FQDN and Key ID.

3.2.3.1.7 IKE Phase

IKE Phase	
Item	Setting
▶ Negotiation Mode	Main Mode ▾
▶ X-Auth	None ▾ X-Auth Account User Name : Password :
▶ Dead Peer Detection (DPD)	☒ Enable Timeout : 180 (seconds) Delay : 30 (seconds)
▶ Phase1 Key Life Time	3600 (seconds) (Max. 86400)

1. **Negotiation Mode:** Choose Main Mode or Aggressive Mode:
Main Mode provides identity protection by authenticating peer identities when pre-shared keys are used. The IKE SA's are used to protect the security negotiations. Aggressive mode will accelerate the establishing speed of VPN tunnel, but the device will suffer from less security in the meanwhile. Hosts in both ends of the tunnel must support this mode so as to establish the tunnel properly.
2. **X-Auth:** For the extended authentication function (XAUTH), the VPN client (or initiator) needs to provide additional user information to the remote VPN server (or Business Security Gateway). The VPN server would reject the connect request from VPN clients because of invalid user information, even though the pre-shared key is correct. This function is suitable for remote mobile VPN clients. You can not only configure a VPN rule with a pre-shared key for all remote users, but you can also designate account / password for specific users that are permitted to establish VPN connection with VPN server. There are 3 roles to let Business Security Gateway behave as for X-Auth authentication, including None, Server and Client. For None role, there is no X-Auth authentication happens during VPN tunnel establishing. For Server role, click "X-Auth Account" button to modify 10 user accounts for user validation during tunnel establishing to VPN server. Finally, for Client role, there are two additional parameters to fill: "User Name" and "Password" for valid user to initiate that tunnel.
3. **Dead Peer Detection:** This feature will detect if remote VPN peer still exists. Delay indicates the interval between detections, and Timeout indicates the timeout of detected to be dead.
4. **Phase 1 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 1 between both end gateways.

3.2.3.1.8 IKE Proposal Definition

IKE Proposal Definition				
ID	Encryption	Authentication	DH Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	☒ Enable
2	AES-auto ▼	MD5 ▼	Group 2 ▼	☒ Enable
3	DES ▼	SHA1 ▼	Group 2 ▼	☒ Enable
4	3DES ▼	SHA1 ▼	Group 2 ▼	☒ Enable

There are 4 IKE proposals can be defined by you and used in IKE phase of negotiation between two VPN peers.

1. **Encryption:** There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192, and AES-256.
2. **Authentication:** There are **five** algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.
3. **DH Group:** There are **nine** groups can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18.
4. **Enable:** Check this box to enable the IKE Proposal during tunnel establishing.

3.2.3.1.9 IPSec Phase

IPSec Phase	
Item	Setting
▶ Phase2 Key Life Time	28800 seconds (Max. 86400)

1. **Phase 2 Key Life Time:** The value of life time represents the life time of the key which is dedicated at Phase 2 between two VPN peers.

3.2.3.1.10 IPSec Proposal Definition

IPSec Proposal Definition				
ID	Encryption	Authentication	PFS Group	Definition
1	AES-auto ▼	SHA1 ▼	Group 2 ▼	☒ Enable
2	AES-auto ▼	MD5 ▼		☒ Enable
3	DES ▼	SHA1 ▼		☒ Enable
4	3DES ▼	SHA1 ▼		☒ Enable

There are 4 IPSec proposals can be defined by you and used in IPSec phase of negotiation between two VPN peers.

1. **Encryption:** There are six algorithms can be selected: DES, 3DES, AES-auto, AES-128, AES-192, and AES-256.
2. **Authentication:** There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512.

3. **PFS Group:** There are nine groups can be selected: None, Group 1 (MODP768), Group 2 (MODP1024), Group 5 (MODP1536) and Group14 ~ 18. Once the PFS Group is selected in one IPSec proposal, the one in other 3 IPSec proposals uses the same choice.
4. **Enable:** Check this box to enable the IKE Proposal during tunnel establishing.

3.2.3.1.11 Manual Proposal

Manual Proposal	
Item	Setting
▶ Outbound SPI	0x
▶ Inbound SPI	0x
▶ Encryption	DES
▶ Authentication	None

When “Manually” key management is used, there are 4 further parameters need to be specified by you and used in IPSec tunnel establishing.

1. **Outbound SPI:** SPI is an important parameter during hashing. Outbound SPI will be included in the outbound packet transmitted from local gateway. The value of outbound SPI should be set in hex formatted.
2. **Inbound SPI:** Inbound SPI will be included in the inbound packet transmitted from remote VPN peer. It will be used to de-hash the coming packet and check its integrity. The value of inbound SPI should be set in hex formatted.
3. **Encryption Algorithm:** There are five algorithms can be selected: DES, 3DES, AES-128, AES-192, and AES-256. Encryption key is used by the encryption algorithm. Its length is 16 in hex format if encryption algorithm is DES or 48 if 3DES. However, AES-128 uses 32 length of hex format, AES-192 uses 48 length of hex format, and AES-256 uses 64 length of hex format. The key value should be set in hex formatted here.
4. **Authentication:** There are five algorithms can be selected: None, MD5, SHA1, SHA2-256 and SHA2-512. Authentication key is used by the authentication algorithm and its length is 32 in hex format if authentication algorithm is MD5 or 40 if SHA1. However, SHA2-256 uses 64 length of hex format. Certainly, its length will be 0 if no authentication algorithm is chosen. The key value should be also set in hex formatted.

3.2.3.2 PPTP

The Point-to-Point Tunneling Protocol (PPTP) is a method for implementing virtual private networks. PPTP uses a control channel over TCP and a GRE tunnel operating

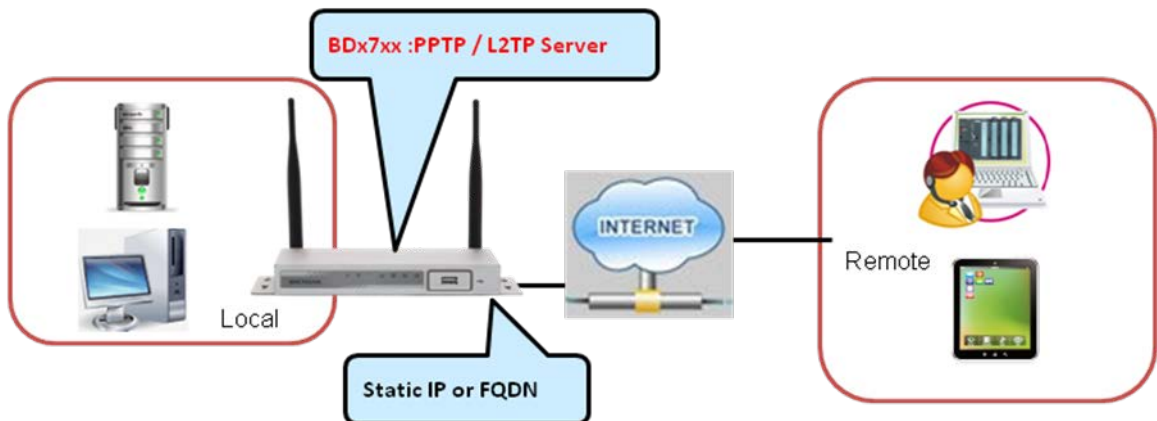
to encapsulate PPP packets. The PPTP specification does not describe encryption or authentication features and relies on the Point-to-Point Protocol being tunneled to implement security functionality. However, the most common PPTP implementation shipping with the Microsoft Windows product families implements various levels of authentication and encryption natively as standard features of the Windows PPTP stack. The intended use of this protocol is to provide security levels and remote access levels comparable with typical VPN products.

3.2.3.2.1 PPTP / L2TP VPN Tunnel Scenarios

There are some common PPTP/L2TP VPN connection scenarios as follows:

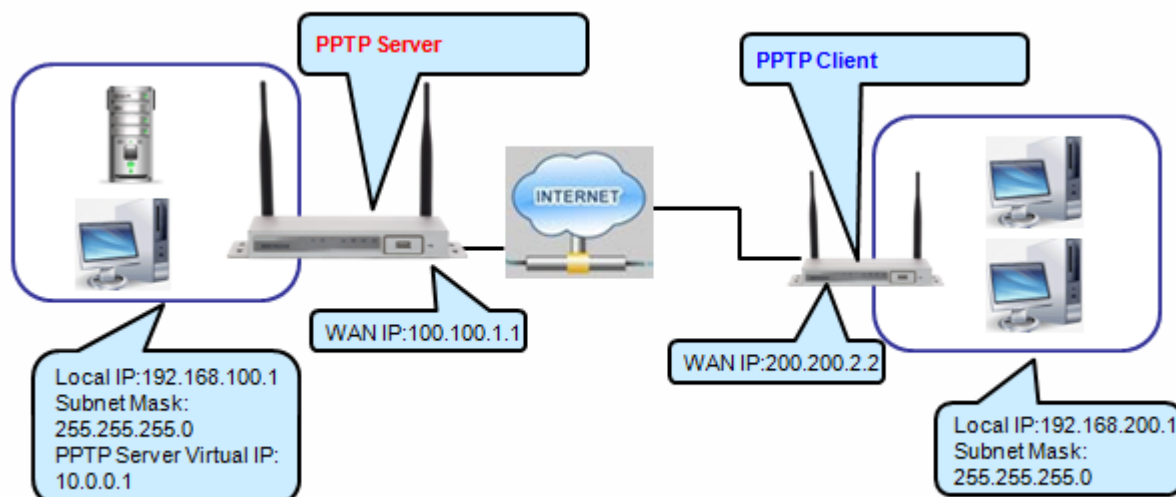
- PPTP / L2TP Server for Remote Mobile Users

The device acts as Server role for remote users to dial in and shares some services in Intranet for them.



- PPTP / L2TP Server / Client Application

The device acts as Server or Client role in SMB Headquarters or Branch Office.



The Business Security Gateway can behave as a PPTP server and a PPTP client at the same time.

Configuration [HELP]	
Item	Setting
PPTP	☒ Enable
Client/Server	Server

1. **PPTP:** Check the “Enable” box to activate PPTP client and server functions.
2. **Client/Server:** Choose Server or Client to configure corresponding role of PPTP VPN tunnels for the Business Security Gateway beneath the choosing screen

3.2.3.2.2 PPTP Server Configuration

The Business Security Gateway can behave as a PPTP server, and it allows remote hosts to access LAN servers behind the PPTP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

PPTP Server Configuration	
Item	Setting
PPTP Server	☒ Enable
Server Virtual IP	192.168.0.1
IP Pool Starting Address	10
IP Pool Ending Address	100
Authentication Protocol	☒ PAP ☒ CHAP ☒ MS-CHAP ☒ MS-CHAP v2
MPPE Encryption	☐ Enable 40bits

1. **PPTP Server:** Enable or disable PPTP server function.

2. **Server Virtual IP:** It is the virtual IP address of PPTP server used in PPTP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.
3. **IP Pool Starting Address:** This device will assign an IP address for each remote PPTP client. This value indicates the beginning of IP pool.
4. **IP Pool Ending Address:** This device will assign an IP address for each remote PPTP client. This value indicates the end of IP pool.
5. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.
6. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.

3.2.3.2.3 PPTP Server Status

The user name and connection information for each connected PPTP client to the PPTP server of the Business Security Gateway will be shown in this table.

PPTP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

1. **Refresh:** To refresh the PPTP Server Status each 2 seconds by clicking on the “Refresh” button.
2. **Disconnect:** To terminate the connection between PPTP server and remote dialing in PPTP clients by clicking on the “Disconnect” button.

3.2.3.2.4 User Account List

You can input up to 10 different user accounts for dialing in PPTP server.

User Account List Add Delete				
ID	User Name	Password	Enable	Actions
1	Test	Test	☒	Edit ☐ Select

1. **Add:** You can add one new user account by clicking on the “Add” button.
2. **Delete:** Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.
3. **Enable:** Check the “Enable” box to validate the user account.
4. **Edit:** You can edit one user account configuration by clicking on the “Edit” button

at the end of each user account list.

3.2.3.2.5 User Account Configuration

Add or edit one user account will activate the “User Account Configuration” screen.

User Account Configuration		
User Name	Password	Account
		☐ Enable
Save		

1. **User Name:** Enter the user name of user account.
2. **Password:** Enter the password of user account.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Save:** To save the user account configuration.

3.2.3.2.6 PPTP Client

The Business Security Gateway also can behave as a PPTP client except PPTP server, and PPTP client tries to establish a PPTP tunnel to remote PPTP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the PPTP server.

PPTP Client Configuration	
Item	Setting
▶ PPTP Client	☒ Enable

1. **PPTP Client:** Enable or disable PPTP client function.

3.2.3.2.7 PPTP Client List & Status

You can add new up to 22 different PPTP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existed tunnel.

PPTP Client List & Status Add Delete Refresh							
ID	PPTP Client Name	Virtual IP	Remote IP/FQDN	Default Gateway/ Gateway/Remote Subnet	Status	Enable	Actions

1. **Add:** You can add one new PPTP client tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Refresh:** Press “Refresh” button to renew PPTP client list and status manually.
4. **Edit:** You can edit one PPTP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

3.2.3.2.8 PPTP Client Configuration

Configuration ▶ IPSec ▶ PPTP ▶ L2TP ▶ GRE	
PPTP Client Configuration	
Item	Setting
▶ PPTP Client Name	PPTP #1
▶ Operation Mode	Always on ▼
▶ Remote IP/FQDN	
▶ User Name	
▶ Password	
▶ Default Gateway/Remote Subnet	Remote Subnet ▼
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable
▶ NAT before Tunneling	☐ Enable
▶ LCP Echo Type	Auto ▼
	Interval seconds Max. Failure Time times
▶ Tunnel	☐ Enable

1. **PPTP Client Name:** The name of this tunnel.
2. **Operation Mode:** Default is “Always on” and other options depend on product models.
3. **Remote IP/FQDN:** The IP address or Domain name of remote PPTP server.
4. **User Name:** The user name which can be validated by remote PPTP server.
5. **Password:** The password which can be validated by remote PPTP server.
6. **Default Gateway/Remote Subnet:** You can choose “Default Gateway” option or “Peer Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this PPTP tunnel if these packets don’t match the Peer Subnet of other PPTP tunnels. There is only one PPTP tunnel to own the “Default Gateway” property. However, when “Peer Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote PPTP server. If an Intranet packet wants to go to this peer subnet, the PPTP tunnel will be established automatically.
7. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote PPTP server.
8. **MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.
9. **NAT before Tunneling:** Check the “Enable” box to let hosts in the Intranet of

Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option can't be enabled.

10. **LCP Echo Type:** Choose the way to do connection keep alive. By default, it is "Auto" option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose "User-defined" option to define the time interval and the retry times by yourself. The last option is "Disable".
11. **Tunnel:** Check the "Enable" box to activate the tunnel.

3.2.3.3 L2TP

In computer networking, Layer 2 Tunneling Protocol (L2TP) is a tunneling protocol used to support virtual private networks (VPNs) or as part of the delivery of services by ISPs. It does not provide any encryption or confidentiality by itself. Rather, it relies on an encryption protocol that it passes within the tunnel to provide privacy.

The Business Security Gateway can behave as a L2TP server and a L2TP client at the same time.

Configuration [HELP]	
Item	Setting
▶ L2TP	☒ Enable
▶ Client/Server	Server ▼

1. **L2TP:** Check the "Enable" box to activate L2TP client and server functions.
2. **Client/Server:** Choose Server or Client to configure corresponding role of L2TP VPN tunnels for the Business Security Gateway beneath the choosing screen.

3.2.3.3.1 L2TP Server Configuration

The Business Security Gateway can behave as a L2TP server, and it allows remote hosts to access LAN servers behind the L2TP server. The device can support four authentication methods: PAP, CHAP, MS-CHAP and MS-CHAP v2. Users can also enable MPPE encryption when using MS-CHAP or MS-CHAP v2.

L2TP Server Configuration	
Item	Setting
▶ L2TP Server	☒ Enable
▶ L2TP over IPsec	☐ Enable Preshare Key (Min. 8 characters)
▶ Server Virtual IP	192.168.10.1
▶ IP Pool Starting Address	10
▶ IP Pool Ending Address	100
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable 40 bits
▶ Service Port	1701

- L2TP Server:** Enable or disable L2TP server function.
- L2TP over IPsec:** L2TP over IPsec VPNs allow you to transport data over the Internet, while still maintaining a high level of security to protect data. Enter a Pre-shared key that system will use it in IPsec tunneling. And when you use some devices, like Apple related mobile devices, you should also know that key to establish L2TP over IPsec tunnels.
- Server Virtual IP:** It is the virtual IP address of L2TP server used in L2TP tunneling. This IP address should be different from the gateway one and members of LAN subnet of Business Security Gateway.
- IP Pool Starting Address:** This device will assign an IP address for each remote L2TP client. This value indicates the beginning of IP pool.
- IP Pool Ending Address:** This device will assign an IP address for each remote L2TP client. This value indicates the end of IP pool.
- Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2.
- MPPE Encryption:** Check the “Enable” box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication method. In the meantime, you also can choose encryption length of MPPE encryption, 40 bits, 56 bits or 128 bits.
- Service Port:** Port number of L2TP server service.

3.2.3.3.2 L2TP Server Status

The user name and connection information for each connected L2TP client to the L2TP server of the Business Security Gateway will be shown in this table.

L2TP Server Status Refresh				
User Name	Remote IP	Remote Virtual IP	Remote Call ID	Actions
No connection from remote				

1. **Refresh:** To refresh the L2TP Server Status each 2 seconds by clicking on the “Refresh” button.
2. **Disconnect:** To terminate the connection between L2TP server and remote dialing in L2TP clients by clicking on the “Disconnect” button.

3.2.3.3.3 User Account List

You can input up to 10 different user accounts for dialing in L2TP server.

User Account List Add Delete				
ID	User Name	Password	Enable	Actions
1	Test	Test	☒	Edit Select

1. **Add:** You can add one new user account by clicking on the “Add” button.
2. **Delete:** Delete selected user accounts by checking the “Select” box at the end of each user account list and then clicking on the “Delete” button.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Edit:** You can edit one user account configuration by clicking on the “Edit” button at the end of each user account list.

3.2.3.3.4 User Account Configuration

Add or edit one user account will activate the “User Account Configuration” screen.

User Account Configuration		
User Name	Password	Account
Test	Test	☒ Enable
Save		

1. **User Name:** Enter the user name of user account.
2. **Password:** Enter the password of user account.
3. **Account:** Check the “Enable” box to validate the user account.
4. **Save:** To save the user account configuration.

3.2.3.3.5 L2TP Client

The Business Security Gateway also can behave as a L2TP client except L2TP server, and L2TP client tries to establish a L2TP tunnel to remote L2TP server. All client hosts in the Intranet of Business Security Gateway can access LAN servers behind the L2TP server.

L2TP Client Configuration	
Item	Setting
L2TP Client	☒ Enable

1. **L2TP Client Configuration:** Enable or disable L2TP client function.

3.2.3.3.6 L2TP Client List & Status

You can add new up to 22 different L2TP client tunnels by clicking on the “Add” button, and modify each tunnel configuration by clicking on the corresponding “Edit” button at the end of each existed tunnel.

L2TP Client List & Status Add Delete Refresh							
ID	L2TP Client Name	Virtual IP	Remote IP/FQDN	Default Gateway/Remote Subnet	Status	Enable	Actions

1. **Add:** You can add one new L2TP client tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Tunnel:** Check the “Enable” box to activate the tunnel.
4. **Edit:** You can edit one L2TP client tunnel configuration by clicking on the “Edit” button at the end of each tunnel list.

3.2.3.3.7 L2TP Client Configuration

L2TP Client Configuration [Help]	
Item	Setting
▶ L2TP Client Name	L2TP #1
▶ Operation Mode	Always on
▶ Remote LNS IP/FQDN	
▶ Remote LNS Port	Auto
▶ User Name	
▶ Password	
▶ Tunneling Password (Optional)	
▶ Default Gateway/Remote Subnet	Remote Subnet
▶ Authentication Protocol	☐ PAP ☐ CHAP ☐ MS-CHAP ☐ MS-CHAP v2
▶ MPPE Encryption	☐ Enable
▶ NAT before Tunneling	☐ Enable
▶ LCP Echo Type	Auto
	Interval 30 seconds Max. Failure Time 6 times
▶ Service Port	Auto 0
▶ Tunnel	☐ Enable

1. **L2TP Client Name:** The name of this tunnel.
2. **Operation Mode:** Default is “Always on” and other options depend on product models.
3. **Remote LNS IP/FQDN:** The IP address or Domain name of remote L2TP server.

4. **Remote LNS Port:** Port number of remote L2TP server.
5. **User Name:** The user name which can be validated by remote L2TP server.
6. **Password:** The password which can be validated by remote L2TP server.
7. **Tunneling Password:** Enter tunneling password if remote L2TP server requests it. It's optional.
8. **Default Gateway/Remote Subnet:** You can choose "Default Gateway" option or "Remote Subnet" option here. When "Default Gateway" is chosen, all traffic from Intranet of Business Security Gateway goes over this L2TP tunnel if these packets don't match the Peer Subnet of other L2TP tunnels. There is only one L2TP tunnel to own the "Default Gateway" property. However, when "Peer Subnet" is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote L2TP server. If an Intranet packet wants to go to this peer subnet, the L2TP tunnel will be established automatically.
9. **Authentication Protocol:** You can choose authentication protocol as PAP, CHAP, MS-CHAP, or MS-CHAP v2. The protocol you choose must be supported by remote L2TP server.
10. **MPPE Encryption:** Check the "Enable" box to activate MPPE encryption. Please note that MPPE needs to work with MS-CHAP or MS-CHAP v2 authentication methods.
11. **NAT before Tunneling:** Check the "Enable" box to let hosts in the Intranet of Business Security Gateway can go to access Internet via remote PPTP server. By default, it is enabled. However, if you want the remote PPTP Server to monitor the Intranet of local Business Security Gateway, the option can't be enabled.
12. **LCP Echo Type:** Choose the way to do connection keep alive. By default, it is "Auto" option that means system will automatically decide the time interval between two LCP echo requests and the times that system can retry once system LCP echo fails. You also can choose "User-defined" option to define the time interval and the retry times by yourself.
13. **Service Port:** Indicate which port on this device is used to connect to remote L2TP server.
14. **Tunnel:** Check the "Enable" box to activate the tunnel.

3.2.3.4 GRE

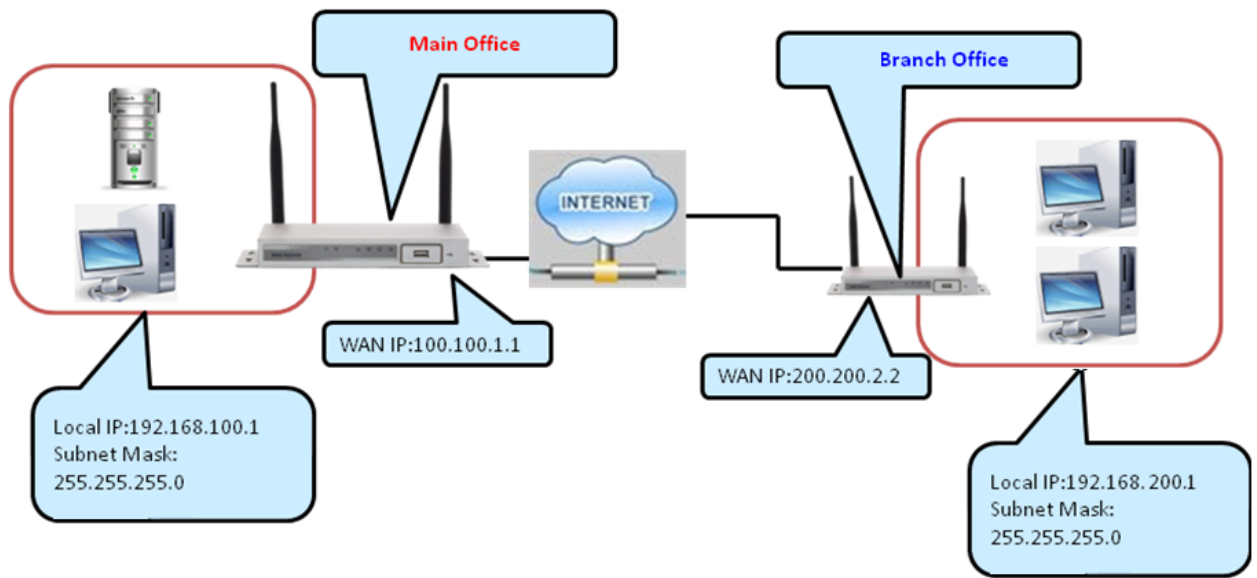
Generic Routing Encapsulation (GRE) is a tunneling protocol developed by Cisco Systems that can encapsulate a wide variety of network layer protocols inside virtual point-to-point links over an Internet Protocol internetwork.

3.2.3.4.1 GRE VPN Tunnel Scenario

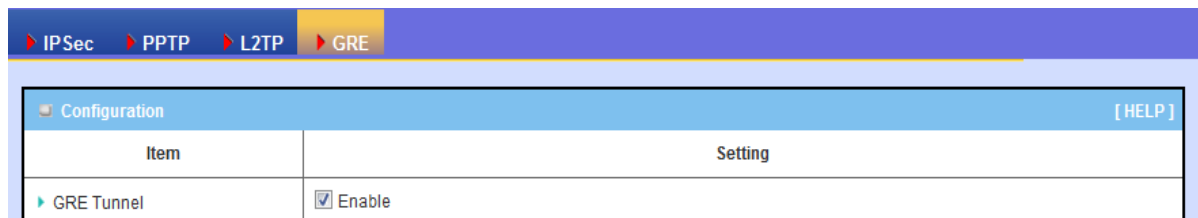
There is one common GRE VPN connection scenario as follows:

- GRE Server / Client Application

The Business Security Gateway acts as GRE Server or Client role in SMB Headquarters or Branch Office.



3.2.3.4.2 GRE Configuration



The screenshot shows the **GRE** configuration page. The navigation bar includes **IPSec**, **PPTP**, **L2TP**, and **GRE**. The main content area is titled **Configuration** and includes a **[HELP]** link. It contains a table with two columns: **Item** and **Setting**. The table has one row: **GRE Tunnel** with the setting ☒ **Enable**.

1. **GRE Tunnel:** Check the “Enable” box to activate the GRE tunnel function.

3.2.3.4.3 GRE Tunnel Definitions

GRE Tunnel Definitions Add Delete										
ID	Tunnel Name	Interface	Operation Mode	Tunnel IP	Remote IP	Key	TTL	Default Gateway/Peer Subnet	Enable	Actions

1. **Add:** You can add one new GRE tunnel by clicking on the “Add” button.
2. **Delete:** Delete selected tunnels by checking the “Select” box at the end of each tunnel list and then clicking on the “Delete” button.
3. **Tunnel:** Check the “Enable” box to activate the GRE tunnel.
4. **Edit:** You can edit one tunnel configuration by clicking the “Edit” button at the end of each tunnel list.

3.2.3.4.4 GRE rule Configuration

GRE Rule Configuration [Help]	
Item	Setting
▶ Tunnel Name	GRE #1
▶ Interface	WAN 1 ▼
▶ Operation Mode	Always on ▼
▶ Tunnel IP	
▶ Remote IP	
▶ Key	
▶ TTL	
▶ Keep alive	☒ Enable Ping IP ▼ Interval 5 (seconds)
▶ Default Gateway/Peer Subnet	Default Gateway ▼ 0.0.0.0/0
▶ DMVPN Spoke	☒ Enable
▶ IPSec Pre-shared Key	(Min. 8 characters)
▶ Tunnel	☒ Enable

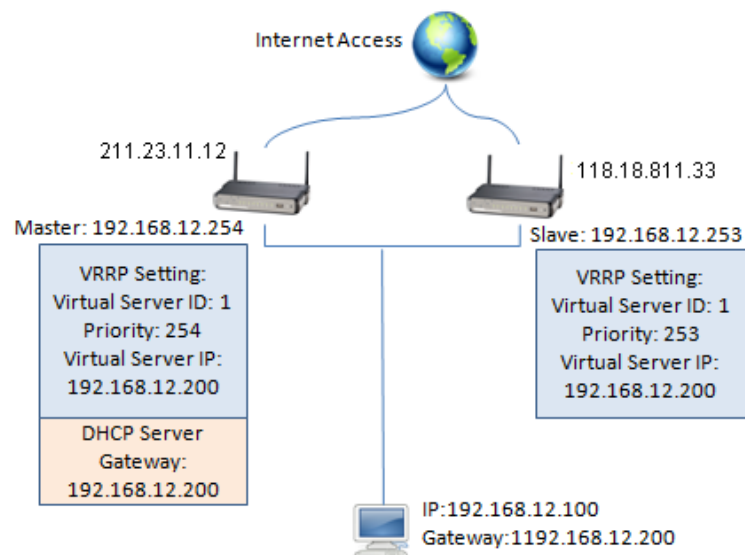
1. **Tunnel Name:** The name of this GRE tunnel.
2. **Interface:** Choose WAN interface for GRE tunnel.
3. **Operation Mode:** Default is “Always on” and other options depend on product models.
4. **Tunnel IP:** The gateway IP address of Business Security Gateway.
5. **Remote IP:** Enter the IP address of remote peer that you want to connect.
6. **Key:** Enter the password to establish GRE tunnel with remote host.
7. **TTL:** Time-To-Live for packets. The value is within 1 to 255. If a packet passes number of TTL routers and still can't reach the destination, then this packet will be dropped.
8. **Keep alive:** Choose the way to do connection keep alive. The keep alive is done by sending ICMP request to a remote host. You need to enter the IP address of remote host and define the time interval of sending ICMP requests.
9. **Default Gateway/Peer Subnet:** You can choose “Default Gateway” option or “Peer Subnet” option here. When “Default Gateway” is chosen, all traffic from Intranet of Business Security Gateway goes over this GRE tunnel if these packets don't match the Peer Subnet of other GRE tunnels. There is only one GRE tunnel to own the “Default Gateway” property. However, when “Peer Subnet” is chosen, peer subnet parameter needs to be filled and it should be the LAN subnet of remote GRE server. If an Intranet packet wants to go to this peer subnet, the GRE tunnel will be established automatically.
10. **DMVPN Spoke:** Check this checkbox to enable DMVPN spoke function.

11. **IPSec Pre-shared Key:** This option is only for DMVPN spoke function. If you enable DMVPN spoke feature, you need to enter same pre-shared key of your existed IPSec tunnel.
12. **Tunnel:** Enable or disable this GRE tunnel.

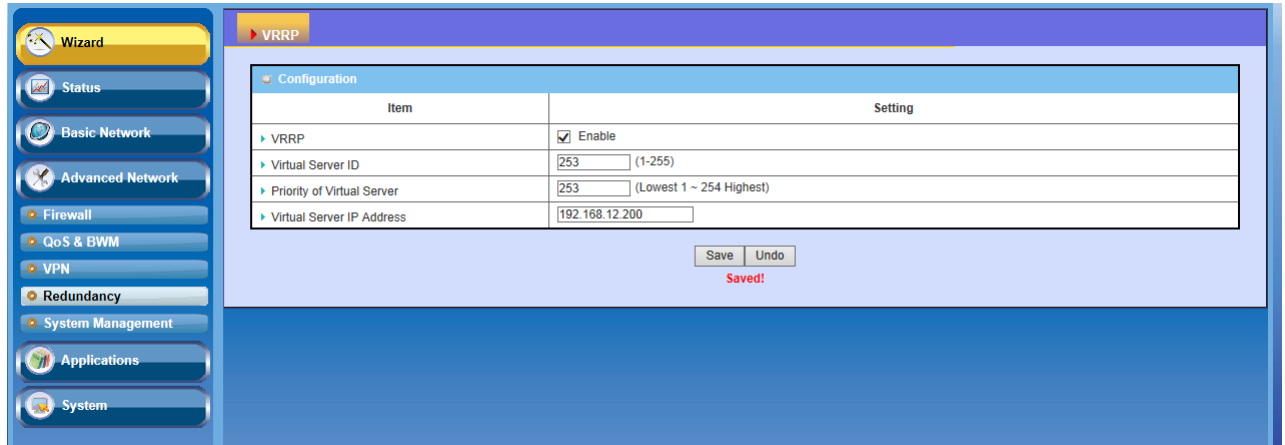
3.2.4 Redundancy

3.2.4.1 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol providing device redundancy. It allows a backup router or switch to automatically take over if the primary (master) router or switch fails. This increases the availability and reliability of routing paths via automatic default gateway selections on an IP network.



The protocol achieves this by creation of virtual routers, which are an abstract representation of multiple routers, i.e. master and backup routers, acting as a group. The default gateway of a participating host is assigned to the virtual router instead of a physical router. If the physical router that is routing packets on behalf of the virtual router fails, another physical router is selected to automatically replace it. The physical router that is forwarding packets at any given time is called the master router.



The screenshot shows the VRRP configuration page. On the left is a sidebar with navigation buttons: Wizard, Status, Basic Network, Advanced Network, Firewall, QoS & BWM, VPN, Redundancy, System Management, Applications, and System. The main area is titled 'VRRP' and contains a 'Configuration' table.

Item	Setting
VRRP	☒ Enable
Virtual Server ID	253 (1-255)
Priority of Virtual Server	253 (Lowest 1 ~ 254 Highest)
Virtual Server IP Address	192.168.12.200

Below the table are 'Save' and 'Undo' buttons. A red 'Saved!' message is displayed below the buttons.

1. **VRRP:** Enable or disable the VRRP function.
2. **Virtual Server ID:** Means Group ID. Specify the ID number of the virtual server. Its value ranges from 1 to 255.
3. **Priority of Virtual Server:** Specify the priority to use in VRRP negotiations. Valid values are from 1 to 254, and a larger value has higher priority.
4. **Virtual Server IP Address:** Specify the IP address of the virtual server.

Click on "Save" to store what you just select or "Undo" to give up.

3.2.5 System Management

This device supports many system management protocols, such as TR-069, SNMP, Telnet with CLI and UPnP. You can finish those configurations in this sub-section.

3.2.5.1 TR-069

TR-069 (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices, like this gateway device. As a bidirectional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). The Security Gateway is such CPE.

Configuration [Help]	
Item	Setting
▶ TR-069	☒ Enable
▶ Interface	WAN-1 ▼
▶ ACS URL	
▶ ACS UserName	
▶ ACS Password	
▶ ConnectionRequest Port	8099
▶ ConnectionRequest UserName	
▶ ConnectionRequest Password	
▶ Inform	☒ Enable Interval 900

TR-069 is a customized feature for ISP; it is not recommend that you change the configuration for this. If you have any problem in using this feature for device management, please contact with your ISP or the ACS provider for help. At the right upper corner of TR-069 Setting screen, one "[Help]" command let you see the same message about that.

3.2.5.2 SNMP

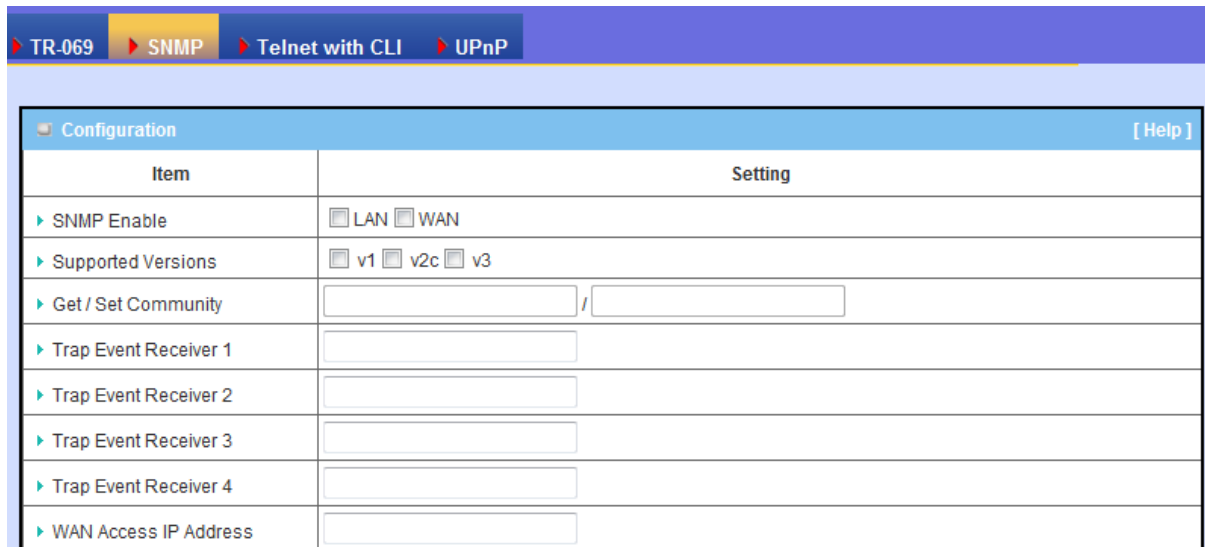
In brief, SNMP, the Simple Network Management Protocol, is a protocol designed to give a user the capability to remotely manage a computer network by polling and setting terminal values and monitoring network events.

In typical SNMP uses, one or more administrative computers, called managers, have the task of monitoring or managing a group of hosts or devices on a computer network. Each managed system executes, at all times, a software component called an agent which reports information via SNMP to the manager.

SNMP agents expose management data on the managed systems as variables. The protocol also permits active management tasks, such as modifying and applying a new configuration through remote modification of these variables. The variables accessible via SNMP are organized in hierarchies. These hierarchies, and other metadata (such as type and description of the variable), are described by Management Information Bases (MIBs).

The device supports several public MIBs and one private MIB for the SNMP agent. The supported MIBs are as follow:

- Supported MIBs
 - MIB-II (RFC 1213, Include IPv6)
 - IF-MIB, IP-MIB, TCP-MIB, UDP-MIB
 - SMIV1 and SMIV2
 - SNMPv2-TM and SNMPv2-MIB
 - AMIB (PROROUTE Private MIB)



Item	Setting
▶ SNMP Enable	☐ LAN ☐ WAN
▶ Supported Versions	☐ v1 ☐ v2c ☐ v3
▶ Get / Set Community	/
▶ Trap Event Receiver 1	
▶ Trap Event Receiver 2	
▶ Trap Event Receiver 3	
▶ Trap Event Receiver 4	
▶ WAN Access IP Address	

1. **SNMP Enable:** You can check “LAN”, “WAN” or both to enable SNMP function. If “LAN” is checked, this device will respond to the request from LAN. If “WAN” is checked, this device will respond to be request from WAN.
2. **SNMP Versions:** Supports SNMP V1, V2c, and v3.
3. **Get / Set Community:** The community of GetRequest that this device will respond. This is a text password mechanism that is used to weakly authenticate queries to agents of managed network devices. The Set community is used for changing configurations on this device.
4. **Trap Event Receiver 1 ~ 4:** Enter the IP addresses or Domain Name of your SNMP Management PCs. You have to specify it, so that the device can send SNMP Trap message to the management PCs consequently.
5. **WAN Access IP Address:** If you want to limit the remote SNMP access to specific computer, please enter the PC`s IP address. The default value is 0.0.0.0, and it means that any internet connected computer can get some information of the device with SNMP protocol.

For SNMP v3, you can setup user profiles to strengthen the way for authentication and encryption.

User Privacy Definition									
ID	User Name	Password	Authentication	Encryption	Privacy Mode	Privacy Key	Authority	Enable	Actions
1			MD5 ▾	DES ▾	authNoPriv ▾		☒ Read ☐ Read/Write	☐	Edit
2			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
3			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
4			MD5	Disable	authNoPriv	Disable	Read	☐	Edit
5			MD5	Disable	authNoPriv	Disable	Read	☐	Edit

- User Name:** user name of this user profile.
- Password:** password of this user profile.
- Authentication:** MD5 or SHA-1 for authentication.
- Encryption:** DES is available for encryption.
- Privacy Mode:** Three options are available for authentication and encryption. Choose “authNoPriv” if you want to do authentication only. Choose “authPriv” if you want to do both of authentication and encryption. If you want to make it simple, choose “noAuthNoPriv” to deactivate authentication and encryption.
- Privacy Key:** Enter the key for encryption. It's only available when Privacy Mode is set to “authPriv”.
- Authority:** Allow this user profile to read information from device only, or change configurations as well (read/write).
- Enable:** Check the box to activate this user profile.
- Actions:** Press “Edit” button to modify user profile.

3.2.5.3 Telnet with CLI

A command-line interface (CLI), also known as command-line user interface, console user interface, and character user interface (CUI), is a means of interacting with a computer program where the user (or client) issues commands to the program in the form of successive lines of text (command lines). The interface is usually implemented with a command line shell, which is a program that accepts commands as text input and converts commands to appropriate operating system functions. Programs with command-line interfaces are generally easier to automate via scripting. The device supports both Telnet and SSH CLI with default service port 2300 and 22, respectively. And it also accepts commands from both LAN and WAN sides.

TR-069 SNMP **Telnet with CLI** UPnP

Configuration	
Item	Setting
Telnet with CLI	LAN : ☒ Enable WAN : ☒ Enable
Connection Type	Telnet : Service Port 2300 ☒ Enable SSH : Service Port 22 ☒ Enable

Save Undo Refresh

Saved!

3.2.5.4 UPnP

UPnP Internet Gateway Device (IGD) Standardized Device Control Protocol is a NAT port mapping protocol and is supported by some NAT routers. It is a common communication protocol of automatically configuring port forwarding. Applications using peer-to-peer networks, multiplayer gaming, and remote assistance programs need a way to communicate through home and business gateways. Without IGD one has to manually configure the gateway to allow traffic through, a process which is error prone and time consuming.

TR-069 SNMP Telnet with CLI **UPnP**

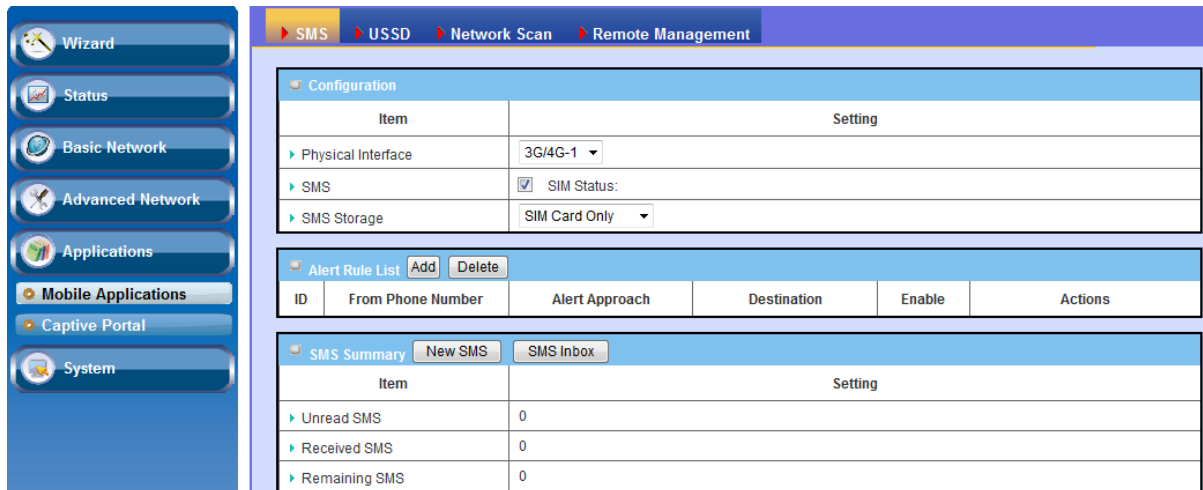
UPnP Setting [Help]	
Item	Setting
UPnP Setting	☐ Enable

Save Undo

This device supports the UPnP Internet Gateway Device (IGD) feature.

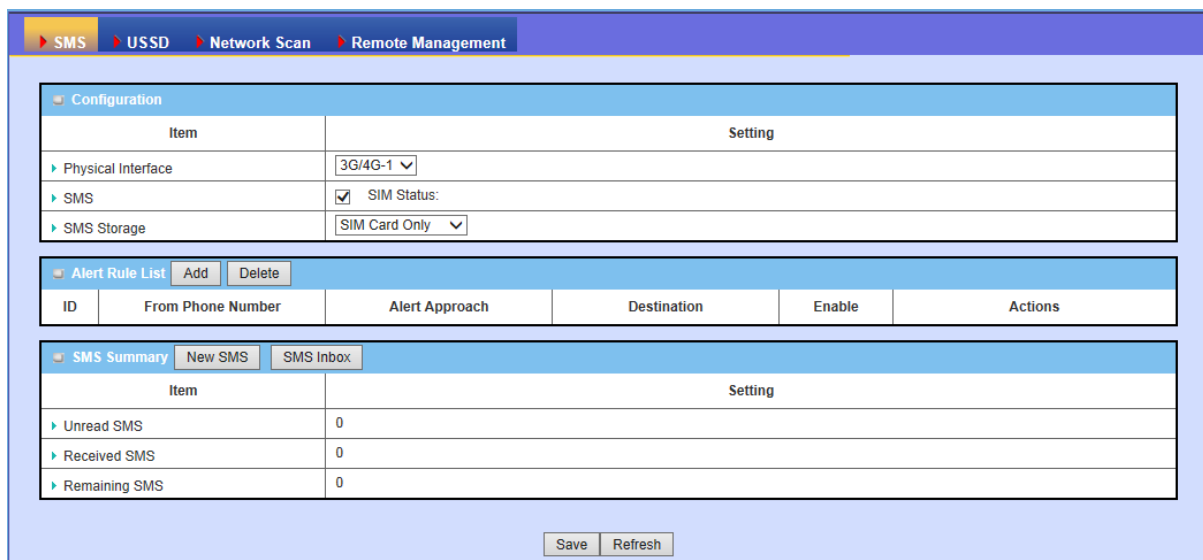
3.3 Applications

In this section you can finish the Mobile Application and Captive Portal settings. For Mobile Application, this device is equipped with a 3G/4G module as WAN interface, and it also provide the SMS, USSD, Network Scan, and Remote Management by SMS. Besides, it also serves as an Internet access gateway. Any client host in the Intranet wants to surf the Internet, the device will redirect the Internet surfing request to an external captive portal Web server for user authentication. If the authentication is successful, the requested client host will be allowed to access Internet by the device.

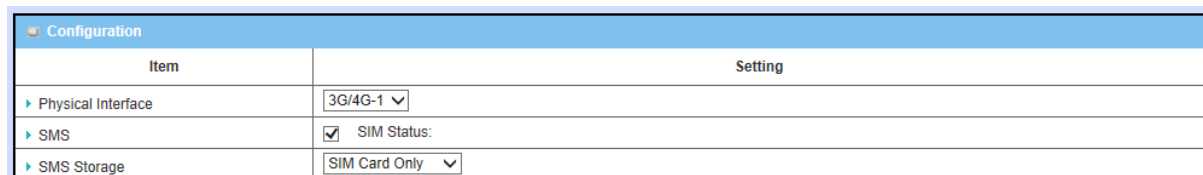


3.3.1 Mobile Application

3.3.1.1 SMS



You can compose new SMS message and check received SMS message on this gateway.



Item	Setting
Physical Interface	3G/4G-1
SMS	☒ SIM Status:
SMS Storage	SIM Card Only

- Physical Interface:** Indicate which 3G/LTE modem is used for SMS feature.
- SMS:** Indicate which SIM card is used for SMS feature.
- SMS Storage:** Select storage for SMS message. This gateway only supports

“SIM Card Only” for SMS storage.

This gateway can forward received SMS message automatically. Press “Add” to add new rule.

Alert Rule List Add Delete															
ID	From Phone Number	Alert Approach	Destination	Enable	Actions										
Alert Rule Configuration Save <table border="1"> <thead> <tr> <th>Item</th> <th>Setting</th> </tr> </thead> <tbody> <tr> <td>▶ From Phone Number</td> <td> </td> </tr> <tr> <td>▶ Alert Approach</td> <td>Auto-forward ▼</td> </tr> <tr> <td>▶ Destination</td> <td> </td> </tr> <tr> <td>▶ Enable</td> <td>☐</td> </tr> </tbody> </table>						Item	Setting	▶ From Phone Number		▶ Alert Approach	Auto-forward ▼	▶ Destination		▶ Enable	☐
Item	Setting														
▶ From Phone Number															
▶ Alert Approach	Auto-forward ▼														
▶ Destination															
▶ Enable	☐														

- 1. From Phone Number:** Indicate phone number of sender.
- 2. Alert Approach:** Decide the way to forward message. You can forward this message to another phone number, or to a mail address, or to a syslog server.
- 3. Destination:** Please enter the phone number of receiver if you choose “Auto-forward”. Or enter a mail address if choosing “By Email”. Or enter the IP address of syslog server if choosing “By Syslog”.
- 4. Enable:** Enable this rule.

SMS Summary

SMS Summary New SMS SMS Inbox	
Item	Setting
▶ Unread SMS	0
▶ Received SMS	0
▶ Remaining SMS	0

- 1. Unread SMS:** Indicate number of unread SMS message.
- 2. Received SMS:** Indicate number of total received SMS message.
- 3. Remaining SMS:** Indicate number of new message can be received because of SMS storage limit.

Create New SMS Message

You can create a new SMS message on this page. After finishing the content of message, and filling with phone number of receiver(s), you can press the “Send” button to send this message out. You can see “Send OK” if the new message has been sent successfully.

New SMS
Send

Item	Setting
Receivers	 (Use '+' for International Format and ';' to Compose Multiple Receivers)
Text Message	Length of Current Input : 0
Result	

Read New SMS Message

You can read, delete, reply, and forward messages in this inbox section.

SMS Inbox List Refresh Delete Close				
ID	From Phone Number	Timestamp	SMS Text Preview	Actions

- Refresh:** You can press “Refresh” button to renew SMS lists.
- Delete, Reply, Forward Messages:** After reading message, you can check the checkbox on the right of each message to delete, reply, or forward this message.

3.3.1.2 USSD

Unstructured Supplementary Service Data (USSD) is a protocol used by GSM cellular telephones to communicate with the service provider's computers. USSD can be used for prepaid callback service, mobile-money services, location-based content services, and as part of configuring the phone on the network.

SMS
USSD
Network Scan
Remote Management

Configuration

Item	Setting
Physical Interface	3G/4G-1 SIM Status:

USSD Profile List
Add
Delete

ID	Profile Name	USSD Command	Comments	Actions
----	--------------	--------------	----------	---------

USSD Request
Send
Clear

Item	Setting
USSD Profile	▼
USSD Command	

Save
Refresh

USSD Configuration

You can compose a USSD message, and sends it to the service provider, where it is received by a computer dedicated to USSD. The answer from this computer is sent back to this device, but it is usually with a very basic presentation.

Configuration	
Item	Setting
Physical Interface	3G/4G-1 SIM Status:

- Physical Interface:** Indicate which 3G/LTE modem is used for USSD feature. And SIM Status indicates which SIM card is used for USSD feature.

USSD Profile List

You can edit USSD profile for some common used command. Press “Add” button to add new profile. And select some existed profiles to delete by clicking on “Delete” button.

USSD Profile List Add Delete				
ID	Profile Name	USSD Command	Comments	Actions

USSD Profile Configuration

USSD Profile Configuration Save	
Item	Setting
Profile Name	
USSD Command	
Comments	

- Profile Name:** Indicate name of this profile.
- USSD Command:** Type USSD command of this profile.
- Comments:** Add comments for this profile.

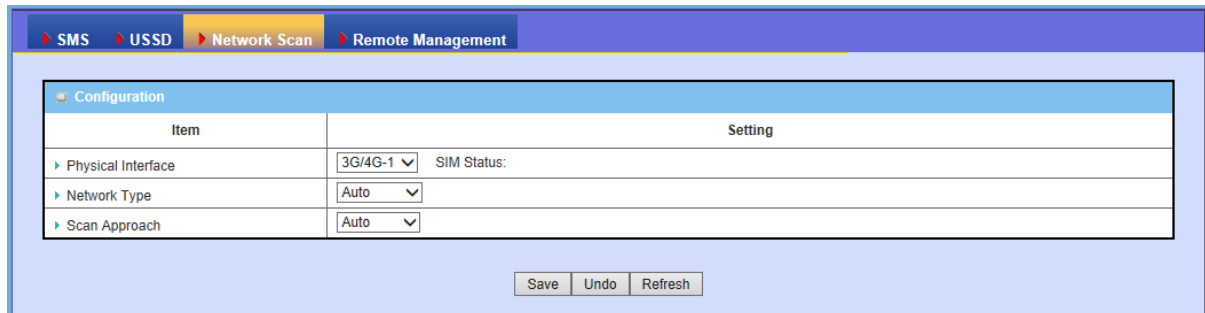
Send USSD Command

USSD Request Send Clear	
Item	Setting
USSD Profile	
USSD Command	

You can select USSD command from existed profile or type command manually. Then press “Send” button to send out USSD command.

3.3.1.3 Network Scan

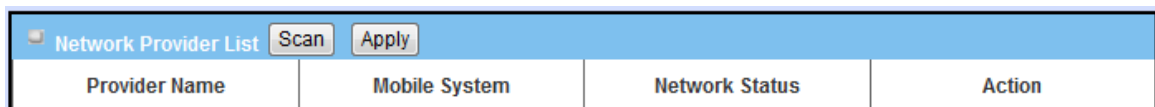
This part is for 3G/LTE cellular network scan. Usually, this part would be done automatically. Manual scan is used for problem diagnosis.



Item	Setting
Physical Interface	3G/4G-1 SIM Status:
Network Type	Auto
Scan Approach	Auto

Save Undo Refresh

- 1. Physical Interface:** Indicate which 3G/LTE modem is used for network scan. And SIM Status indicates which SIM card is used to Network Scan.
- 2. Network Type:** Set network type of network scan. You can choose “2G Only”, “3G Only”, “LTE Only”, or “Auto”.
- 3. Scan Approach:** You can choose “Auto” or “Manually”. If you choose “Manually”, press “Scan” button to scan cellular network nearby in your environment and select one network provider to apply by clicking on the “Apply” button.



Provider Name	Mobile System	Network Status	Action
---------------	---------------	----------------	--------

Note. Incorrect setting here may cause 3G/LTE connection problems.

3.3.1.4 Remote Management

This part is for remote management functions that are done by text SMS (Short Message Service). Users can send certain SMS to this gateway to activate some actions, such as connect/disconnect/reconnect WAN connection or reboot the system. Besides, gateway can also send SMS to users to alert some events automatically.

Management Settings	
Item	Setting
Remote Management via SMS	☒ Enable ☐ Disable
Delete SMS for Remote Management	☒ Enable ☐ Disable
Security Key	SKey
Command Settings	
Item	Setting
Status	☐ Enable ☒ Disable
Connect	☐ Enable ☒ Disable
Disconnect	☐ Enable ☒ Disable
Reconnect	☐ Enable ☒ Disable
Reboot	☐ Enable ☒ Disable
Notification Settings	
Item	Setting
WAN Link Down	☐ Enable ☒ Disable
WAN Link Up	☐ Enable ☒ Disable
Secondary WAN Link is Up	☐ Enable ☒ Disable
Secondary WAN Link is Down	☐ Enable ☒ Disable
Access Control List	
Item	Setting
Access Control	☐ Enable ☒ Disable
Phone 1	 ☐ Management ☐ Notification
Phone 2	 ☐ Management ☐ Notification
Phone 3	 ☐ Management ☐ Notification
Phone 4	 ☐ Management ☐ Notification
Phone 5	 ☐ Management ☐ Notification

Save Undo Reboot

Management Settings

Management Settings	
Item	Setting
Remote Management via SMS	☒ Enable ☐ Disable
Delete SMS for Remote Management	☒ Enable ☐ Disable
Security Key	SKey

- 1. Remote Management via SMS:** Check this to enable this function.
- 2. Delete SMS for Remote Management:** This device will delete received SMS message that is for remote management purpose if enabling this option. This option can prevent storage space of SIM card from being occupied continuously. If SIM storage is full, this gateway can't receive any new SMS.
- 3. Security Key:** This security key will be used for authentication when this gateway receives SMS command. Users need to type this key first and then followed by a command. There should be a "blank" between key and command (e.g. 1234 reboot). If this field is empty, users just need to type command without adding any key information.

Note. If security key is empty, access control needs to be activated. The security key can be empty if access control is activated.

Command Settings

Command Settings	
Item	Setting
Status	☒ Enable ☐ Disable
Connect	☒ Enable ☐ Disable
Disconnect	☒ Enable ☐ Disable
Reconnect	☒ Enable ☐ Disable
Reboot	☒ Enable ☐ Disable

1. **Status:** Enable it, and you can send command “status” to query WAN connection status. For 3G/LTE WAN, router will send back WAN IP address, network name, network type, and connection time via SMS. For Ethernet WAN, router will send back WAN IP address and connection time via SMS. The content would be similar to following format:

WAN IP: [xxx.xx.xxx.xx]

Network: [carrier name] (for wireless WAN only)

Type: [GPRS, WCDMA, HSPA, HSPA+, LTE] (for wireless WAN only)

Conn. Time: [connection time]

2. **Connect:** Enable it, and you can send command “**connect**” to start WAN connection.
3. **Disconnect:** Enable it, and you can send command “**disconnect**” to disconnect WAN connection.
Note. If this gateway receives “disconnect” command from SMS, it won’t try to connect again no matter WAN connection mode is set to auto-reconnect.
4. **Reconnect:** Enable it, and you can send command “**reconnect**” to disconnect WAN connection, and start WAN connection again immediately.
5. **Reboot:** Enable it, and you can send command “**reboot**” to restart router.

****All management commands are not case sensitive****

Notification Settings

Notification Settings	
Item	Setting
▶ WAN Link Down	☒ Enable ☐ Disable
▶ WAN Link Up	☒ Enable ☐ Disable
▶ Secondary WAN Link is Up	☒ Enable ☐ Disable
▶ Secondary WAN Link is Down	☒ Enable ☐ Disable

1. **WAN Link Down:** Enable it, and this gateway will send a message to users if primary WAN connection is dropped.
2. **WAN Link Up:** Enable it, and this gateway will send a message to users if WAN connection is established. This message will also include WAN IP address.
3. **Secondary WAN is Up:** Enable it, and this gateway will send a message to users if secondary WAN is connected. This message will also include WAN IP address.
4. **Secondary WAN is Down:** Enable it, and this gateway will send a message to users if secondary WAN is disconnected.

Access Control List

Access Control List	
Item	Setting
▶ Access Control	☒ Enable ☐ Disable
▶ Phone 1 09376xxxx	☒ Management ☒ Notification
▶ Phone 2 09116xxxx	☐ Management ☒ Notification
▶ Phone 3	☐ Management ☐ Notification
▶ Phone 4	☐ Management ☐ Notification
▶ Phone 5	☐ Management ☐ Notification

- 1. Access Control:** Users can decide which phone number can send commands to this gateway or receive notifications when enable this option.
- 2. Phone 1~5:** For security concern, this gateway won't deal with the command if that phone number is not in the list even the security key is correct. The phone number must be with the international prefix (i.e. +886939123456). You can also assign specific phone number can send command and/or also can receive notifications.

3.3.2 Captive Portal

3.3.2.1 Captive Portal Configuration

Captive Portal Configuration	
Item	Setting
▶ Captive Portal	☐ Enable
▶ WAN Interface	WAN-1
▶ Authentication Server	External RADIUS Server
▶ UAM Server	☐ Enable Select from External Server List

The gateway supports the Captive Portal function, including external captive portal. For external captive portable, you must specify external RADIUS (Remote Authentication Dial In User Service) server and external UAM (Universal Access Method) server.

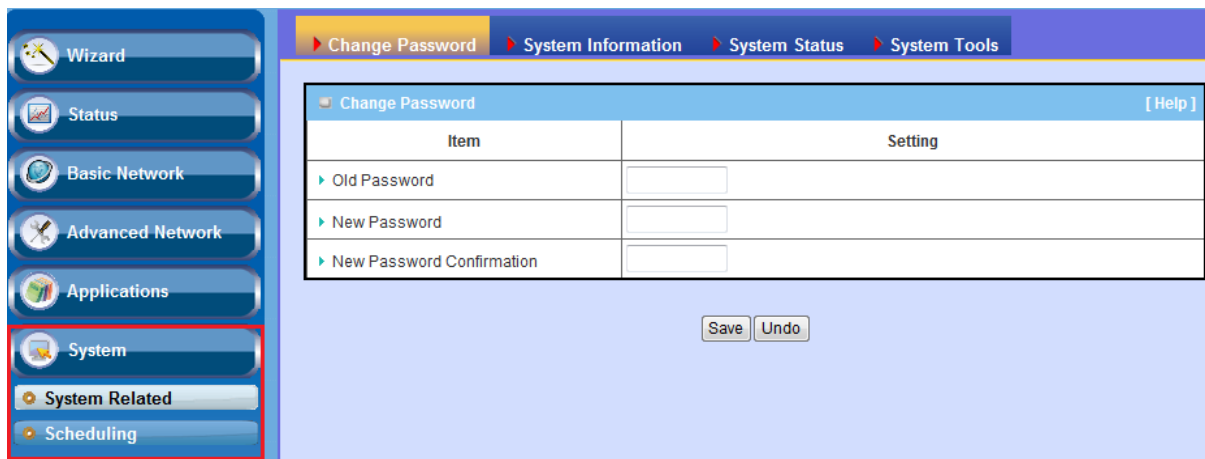
External Captive Portal

Before enabling external Captive Portal function, please go to **System >> External Servers** to define some external server objects, like RADIUS server and UAM server. Then configure Captive Portal function in this page to specific WAN Interface, select external Authentication Server and UAM Server from the pre-defined external server object list.

NOTE: All Internet Packets will forward to Captive Portal Web site of the gateway when enabled this feature. Please make sure that you had one account and password.

3.4 System

In the System section you can see system related information and system logs, use system tools for system update and do some network tests. Besides, you can also define some time scheduling rules here to be applied at various applications in the device system. Administrator Time-out in seconds defines the idle time-out for administrator to configure the device by using Web UI.

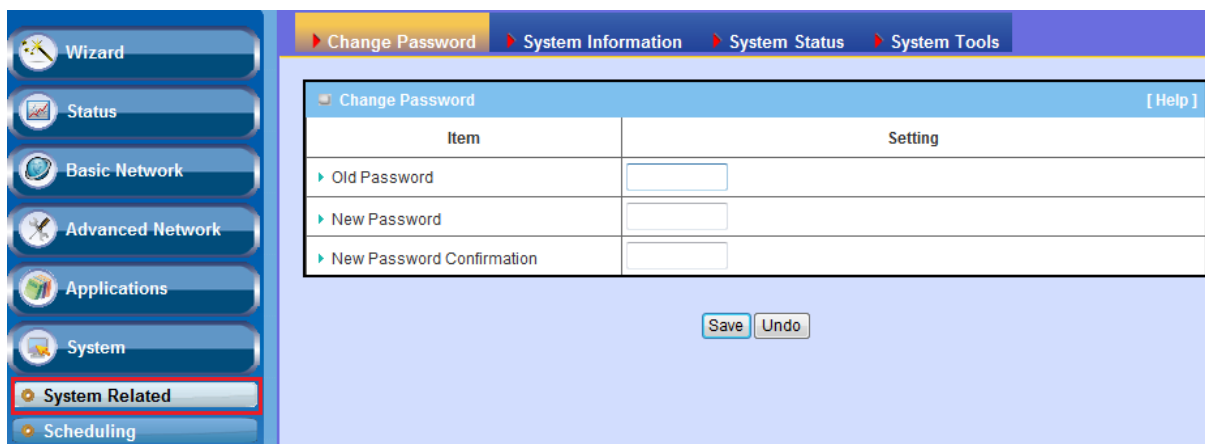


Item	Setting
Old Password	
New Password	
New Password Confirmation	

Save Undo

3.4.1 System Related

In this section, you can change login password, view system information and status, and using several system tools.



Item	Setting
Old Password	
New Password	
New Password Confirmation	

Save Undo

3.4.1.1 Change Password

You can change the System Password here. We **strongly** recommend you to change

the system password for security reason. Click on “Save” to store your settings or click “Undo” to give up the changes.

Change Password [Help]	
Item	Setting
▶ Old Password	
▶ New Password	
▶ New Password Confirmation	

- 1. Old Password:** Input the old password of administrator.
- 2. New Password:** Input the new password of administrator for future logging in. Certainly, once the password is changed successfully, system will ask you login again with new password.
- 3. New Password Confirmation:** Re-type new password again here. It must be the same as the one in “New Password”; otherwise, an error message will be shown out.

3.4.1.2 System Information

You can view the System Information in this page. It includes the WAN Type, Display Time and Modem Information. But the modem information will be existed only at the models with embedded modems, like ADSL modem and 3G/LTE modem. Press “Refresh” button to get updated system information.

System Information	
Item	Setting
▶ WAN Type	Dynamic IP
▶ Display Time	Thu, 01 Jan 1970 01:02:58 +0000

3.4.1.3 System Status

You can view the System Logs in Web UI. You also can send the logs to specific email accounts periodically or instantly by clicking on the “Email Now” command button.

System Web Log View Email Now	
Item	Setting
▶ Web Log	☒ System ☒ Attacks ☒ Drop ☐ Debug Categories
▶ Email Alert	☐ Enable Server List: --- Option --- Email Addresses: E-mail subject:
▶ Syslogd	☐ Enable Server

- Web Log:** You can select the log types to be collected in the web log area. There are “System”, “Attacks”, “Drop”, and “Debug” types for you to select.
- Email Alert:** This device can also export system logs via sending emails to specific recipients. The items you have to setup include:
 - **Enable:** Enable email alert function.
 - **SMTP Server: Port:** Input the SMTP server IP and port, which are connected with ':'. If you do not specify port number, the default value is 25.
For example, "mail.your_url.com" or "192.168.1.100:26".
 - **E-mail Addresses:** The recipients are the ones who will receive these logs. You can assign more than 1 recipient, using ';' or ',' to separate these email addresses.
 - **E-mail Subject:** The subject of email alert is optional.

Press “Email Now” to send system logs immediately.
- Syslogd:** Enable this function to send system logs to remote syslog server periodically. Please enter the IP address of remote syslog server.

3.4.1.4 System Tools

The device supports many system tools, including system time configuration, FW upgrading, system rebooting, system resetting to default, waking on LAN and configuration settings backup.

System Tools	
Item	Setting
System Time	Configure Sync with Time Server Sync with my PC (Tuesday July 22, 2014 10:44:21)
FW Upgrade	FW Upgrade
Ping Test	Host IP: Interface: Auto Ping
Tracert Test	Host IP: Interface: Auto UDP Traceroute
Reboot	Now Reboot
Reset to Default	Reset
Wake on LAN	Wake up
Backup Configuration Settings	Backup

System Time

There are three approaches to setup the system time. Before the process, some basic information must be filled by clicking on the “Configure” command button. Basic information includes following items:

System Time Configuration	
Item	Setting
Time Zone	* Not yet configured! The default is GMT+00:00
Auto-synchronization	☒ Enable Time Server: Available Time Servers (RFC-868): Auto
Daylight Saving Time	☐ Enable
Set Date & Time Manually	2014 / July / 04 (Year/Month/Day) 17 : 40 : 50 (Hour:Minute:Second)

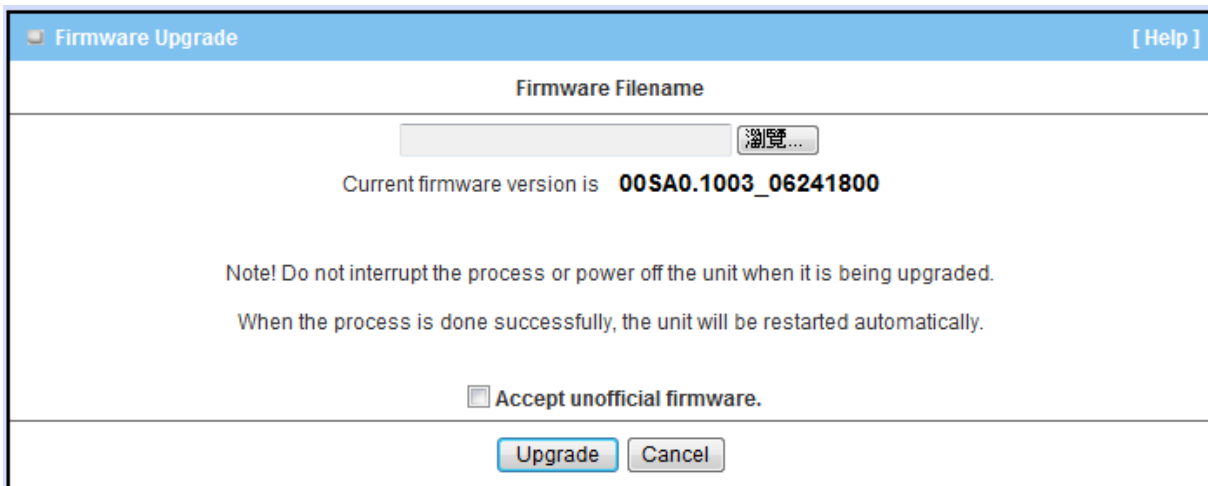
- Time Zone:** Select a time zone where this device locates.
- Auto-synchronization:** Check the “Enable” checkbox to enable this function. Besides, you can select a NTP time server to consult UTC time from the available list and by default, it is “Auto” to let system query pre-defined NTP servers for the system time one after one.
- Daylight Saving Time:** Check the “Enable” checkbox to enable this function.
- Set Date & Time Manually:** Set the date and time for system by manual. But Auto-Synchronization must be unchecked beforehand to do it.

Above is the first way to setup system date and time. That is, it is the manual way. The second way is “Sync with Timer Server”. Based on your selection of time server in basic information configuration, system will communicate with time server by NTP Protocol to get system date and time after you click on the button. The last way is

“Sync with my PC”. Click on the button to let system synchronizes its date and time to the ones of the configuration PC.

FW Upgrade

If new firmware is available, you can upgrade router firmware through the WEB GUI here. After clicking on the “FW Upgrade” command button, you need to specify the file name of new firmware by using “Browse” button, and then click “Upgrade” button to start the FW upgrading process on this device. If you want to upgrade a firmware which is from GPL policy, please check “Accept unofficial firmware”.



The screenshot shows the 'Firmware Upgrade' web interface. At the top, there's a blue header with 'Firmware Upgrade' and a '[Help]' link. Below the header, there's a section titled 'Firmware Filename' with a text input field and a '浏览...' (Browse) button. Underneath, it states 'Current firmware version is 00SA0.1003_06241800'. A note in red text says: 'Note! Do not interrupt the process or power off the unit when it is being upgraded. When the process is done successfully, the unit will be restarted automatically.' Below the note, there's a checkbox labeled 'Accept unofficial firmware.' At the bottom, there are two buttons: 'Upgrade' and 'Cancel'.

NOTE. PLEASE DO NOT TURN THE DEVICE OFF WHEN UPGRADE IS PROCEEDING.

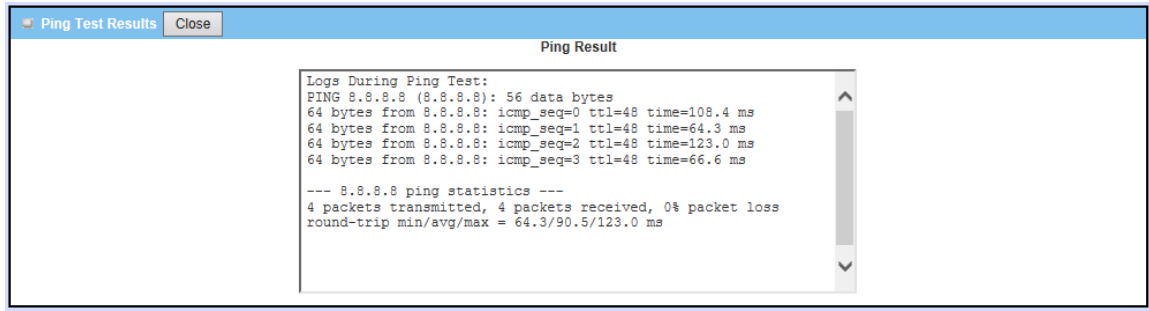
Ping Test

This allows you to specify an IP / FQDN and the test interface, so system will try to ping the specified device to test whether it is alive after clicking on the “Ping” button. A test result window will appear beneath it. There is a “Close” command button there can let the test result windows disappear.



The screenshot shows the 'Ping Test' web interface. It has a tab labeled 'Ping Test'. To the right of the tab, there's a 'Host IP:' label followed by a text input field. Next to it is an 'Interface:' label followed by a dropdown menu currently set to 'Auto'. To the right of the dropdown is a 'Ping' button.

1. **Host IP:** Input the IP address of destination host.
2. **Interface:** Choose which WAN interface will be used for Ping test.
3. **Ping button:** Start to send ICMP packet and system will show the Ping Test Results window as below. Close the window by clicking on the “Close” button.

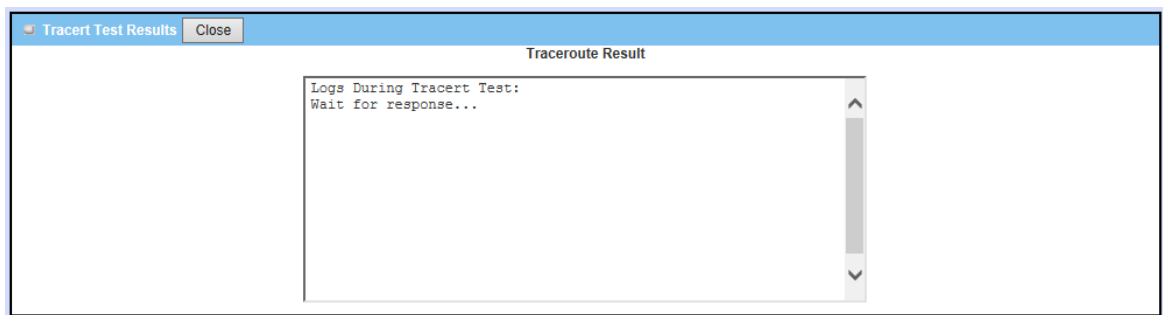


Tracert Test

Traceroute is a network diagnostic tool for displaying the route (path) and measuring transit delays of packets across an IP network. Traceroute proceeds unless all (three) sent packets are lost more than twice, then the connection is lost and the route cannot be evaluated. Ping, on the other hand, only computes the final round-trip times from the destination point. First, you need to specify an IP / FQDN, the test interface and used protocol number. Used protocol number is either “UDP” or “ICMP”, and by default, it is “UDP”. Then, system will try to trace the specified device to test whether it is alive after clicking on the “Traceroute” button. A test result window will appear beneath it. There is a “Close” command button there can let the test result windows disappear.

▶ Tracert Test	Host IP:	Interface: Auto	UDP	Traceroute
----------------	-------------------------------	--	----------------------------------	------------

1. **Host IP:** Input the IP address of destination host.
2. **Interface:** Choose which WAN interface will be used for Tracert test.
3. **Ping button:** Start Tracert test and system will show the Tracert Test Results window as below. Close the window by clicking on the “Close” button.



Reboot

You can reboot this device immediately by clicking the “Reboot” button.

▶ Reboot	Now	Reboot
----------	----------------------------------	--------

Or you can also set time schedule to do reboot periodically.

▶ Reboot	Time Schedule ▼	(0) Always ▼
----------	-----------------	--------------

Reset to Default

You can reset this device to factory default settings by clicking the “Reset” button.

Wake on LAN

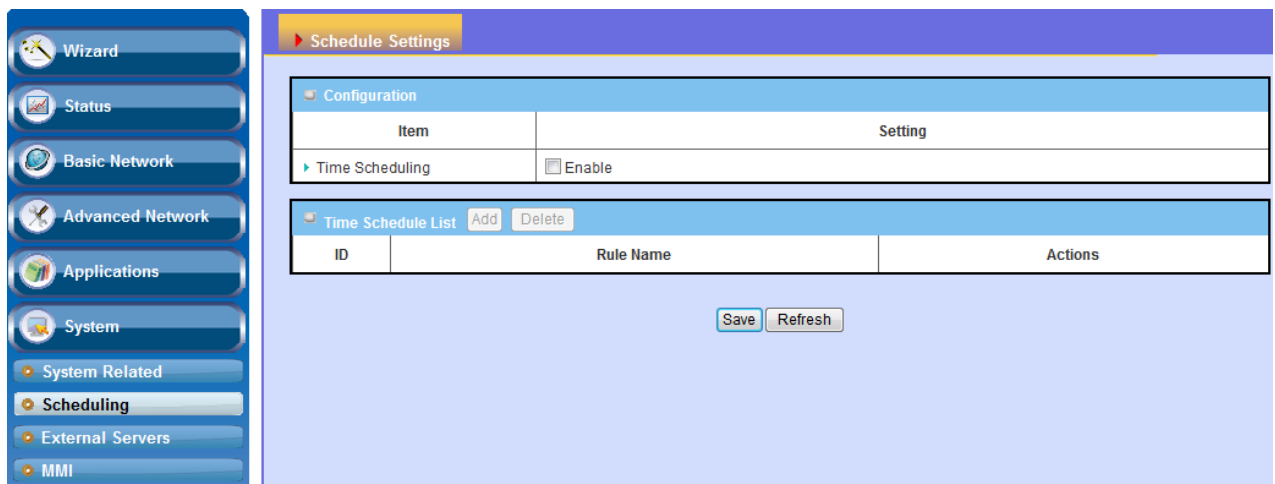
Wake on LAN (WOL) is an Ethernet networking standard that allows a computer to be turned on or awakened by a network message. You can specify the MAC address of the computer, in your LAN network, to be remotely turned on by clicking on the “Wake up” command button.

Backup Configuration Settings

You can backup your settings by clicking the “Backup” button and save it as a bin file. Once you want to restore these settings, please click Firmware Upgrade button and use the bin file you have saved.

3.4.2 Scheduling

You can set the schedule time to decide which service will be turned on or off. The added rules will be listed.



- 1. Time Scheduling:** Enable or disable the scheduling function.
- 2. Add New Rule:** Click the “Add” button to create a schedule rule. When the next dialog popped out you can edit the Name of Rule, Policy, and set the schedule time (Week day, Start Time, and End Time). In a schedule rule, it collects 8 time periods to organize it. You also can specify the rule is to define the enable timing (“Inactive except the selected days and hours below”) or disable timing (“Active except the selected days and hours below”).

Schedule Settings

Time Schedule Configuration

Item	Setting
▶ Rule Name	
▶ Rule Policy	Inactivate ▼ the Selected Days and Hours Below

Time Period Definition

ID	Week Day	Start Time (hh:mm)	End Time (hh:mm)
1	-- choose one -- ▼		
2	-- choose one -- ▼		
3	-- choose one -- ▼		
4	-- choose one -- ▼		
5	-- choose one -- ▼		
6	-- choose one -- ▼		
7	-- choose one -- ▼		
8	-- choose one -- ▼		

Afterwards, click “save” to store your settings or click “Undo” to give up the changes.

3.4.3 External Servers

This device supports six types of external server objects to be created. They are Email Server objects, Syslog Server objects, RADIUS Server objects, Active Directory Server objects, LDAP Server objects and UAM Server objects. These objects can be used in other applications of system, like system log emailing to email server or sending to syslog server in System >> System Related >> System Status, captive portable function in Applications >> Captive Portable, and SMS forwarding to email server or syslog server in Applications >> Mobile Applications >> SMS. Above usage examples depend on the provided functions of different product models.

External Servers

External Server List
Add Delete

ID	Server Name	Server IP/FQDN	Server Port	Server Type	Enable	Setting
External Server Configuration Save						
Item		Setting				
Server Name						
Server IP/FQDN						
Server Port						
Server Type		Email Server User Name: Password:				
Server		☐ Enable				

3.4.3.1 External Server List

External Server List can show the list of all defined external server objects and their attributes in this window. You can add one new external server object by clicking on the “Add” command button. But also you can modify some existed external server objects by clicking corresponding “Edit” command buttons at the end of each object record in the External Server List. Besides, unnecessary objects can be removed by checking the “Select” box for those objects and then clicking on the “Delete” command button at the External Server List caption.

External Server List Add Delete						
ID	Server Name	Server IP/FQDN	Server Port	Server Type	Enable	Setting
1	JPEmailAccount	email.amit.com.tw	25	undefined	☒	Edit ☒ Select
2	JPEmailAccount	email.amit.com.tw		Email Server	☒	Edit ☐ Select

- Add:** Click on the button to add one external server object.
- Delete:** Click on the button to delete the external server objects that are specified in advance by checking on the “Select” box of those objects.
- Edit:** Click on the button to edit the external server object.
- Select:** Select the external server object to delete.

3.4.3.2 External Server Configuration

External Server Configuration
Save

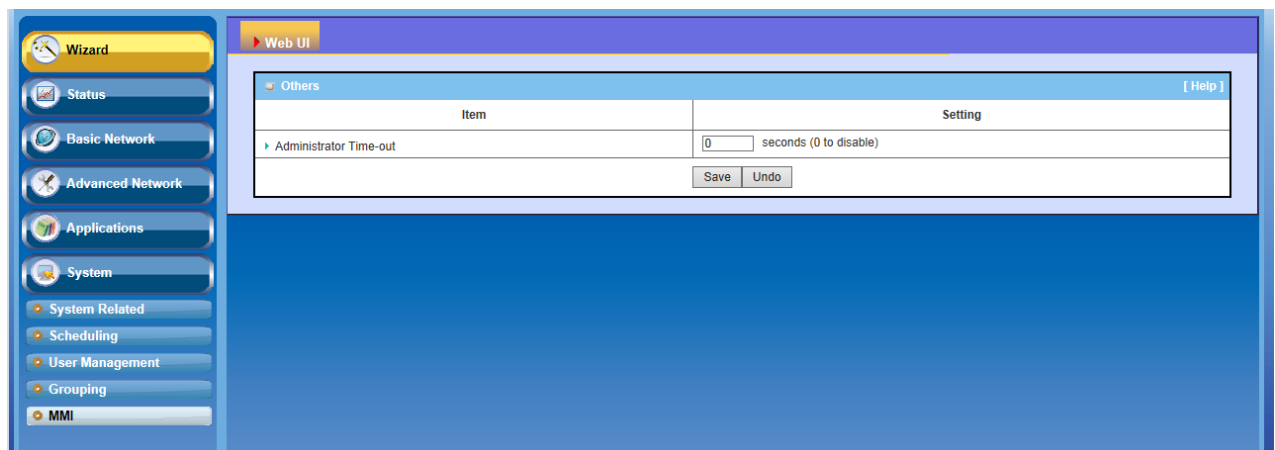
Item	Setting
Server Name	JPEmailAccount
Server IP/FQDN	email.amit.com.tw
Server Port	
Server Type	Email Server User Name: jp Password:
Server	☒ Enable

- Server Name:** Define the name of external server object.

2. **Server IP/FQDN:** Specify the IP address or domain name of external server.
3. **Server Port:** Specify the service port of external server.
4. **Server Type:** Select one server type from the option list of “Email Server”, “Syslog Server”, “RADIUS Server”, “Active Directory Server”, “LDAP Server” and “UAM Server”. Based on your selection, there are several parameters need to specify. When you select “Email Server” option for the Server Type, you must specify two more parameters, “User Name” and “Password”. When “Syslog Server”, no more parameter is required. When “RADIUS Server”, you can specify primary RADIUS server and secondary RADIUS server for redundancy. For each server, following parameters need to be specified: Shared Key, Authentication Protocol (CHAP or PAP), Session Timeout (1~60 Mins) and Idle Timeout (1~15 Mins). When “Active Directory” Server, you must specify one more parameter, “Domain”. When “LDAP” Server, one more parameter, Base Domain Name. When “NT Domains” Server, one more parameter: “Workgroup”. When “UAM” Server, following parameters must be provided: “Login URL”, “Shared Secret”, “NAS/Gateway ID”, “Location ID” and “Location Name”. Among them, Location Name is optional.
5. **Server:** Check the “Enable” box to activate the external server object.

3.4.4 MMI

3.4.4.1 Web UI



You can set UI administration time-out duration in this page. If the value is “0”, means the time-out is unlimited.

Additional Information

For support please contact your supplier in the first instance.